

Eesti elanike küberturvaline käitumine ja küberkäitumise püsiv mõjutamine

uuringuaruanne

2025

praxis | mõttekoda



RIIGI INFOSÜSTEEMI AMET

Uuringu tellis Riigi Infosüsteemi Amet.

Autorid:

Marleen Allemann

Tali Kletter

Elisabeth Kendrali

Uuringu valmimisse andsid olulise panuse ka Eve Mägi ja Liisa Past.

Täname kõiki neid inimesi, kes intervjuudes osalemisega aitasid kaasa uuringu valmimisele. Samuti täname meeldiva koostöö eest tellija esindajaid.

Väljaandes sisalduva teabe kasutamisel palume viidata allikale:

Allemann, M., Kletter, T., Kendrali, E. (2025). *Eesti elanike küberturvaline käitumine ja küberkäitumise püsiv mõjutamine*. Tallinn: SA Mõttekoda Praxis.

ISBN 978-9949-662-55-5 (pdf)

Sisukord

Kokkuvõte ja peamised soovitused	5
Executive summary and main recommendations	9
Kasutatud lühendid ja terminoloogia	13
Sissejuhatus	14
1. Küberturvalise käitumise edendamine Eestis	17
1.1. Küberturvalise käitumise edendamisega seotud osapooled ja nende senine tegevus	17
1.2. Praeguse korralduse tugevused ja kitsaskohad	20
2. Eesti elanike küberkäitumine	24
2.1. Kas küberturvalisus on inimestele oluline ja kui palju nad selle peale mõtleavad?	24
2.2. Milline on inimeste küberteadlikkus ja kas see on aja jooksul muutunud?	25
2.2.1. Inimeste küberteadlikkus ja võimekus	25
2.2.2. Inimeste küberteadlikkuse ja -käitumise muutus ajas	27
2.3. Millised on inimeste harjumused ja põhimõtted oma turvalisuse tagamiseks?	29
2.3.1. Harjumused ja põhimõtted, mida turvalisuse nimel järgitakse	29
2.3.2. Teenused ja tegevused, mille puhul peetakse turvalisust rohkem silmas	33
2.4. Kus on inimeste küberkäitumises vajakajäämised?	36
2.5. Mis ajendab inimesi küberturvaliselt käituma – või mitte?	39
2.5.1. Ajendid küberturvaliseks käitumiseks	39
2.5.2. Ajendid küberhaavatavaks käitumiseks	42
3. Eesti elanike küberkäitumise mõjutamine: inimeste endi vaade	53
3.1. Kust saavad inimesed küberturvalisusalast infot?	53
3.2. Kas küberturvalisusalast infot on inimeste hinnangul piisavalt ja mis teemadel tuleks seda lisaks jagada?	57
3.2.1. Info piisavus	57
3.2.2. Teemad, millest tahaks rohkem teada	59
3.3. Mis motiveeriks inimesi küberturvalisusele rohkem tähelepanu pöörama?	63
3.3.1. Inimeste sisemist motivatsiooni tõstvad tegurid	64
3.3.2. Välised motivaatorid	67
3.4. Kuidas võiks inimeste küberteadlikkust ja -käitumist edendada?	70

3.4.1. Milliseid kanaleid/formaate/tegevusi võiks kasutada?	70
3.4.2. Millised sõnumid ja kõneisikud võiksid inimesi kõnetada?	83
4. (Küber)käitumist püsivalt mõjutavad sekkumised ja nende rakendatavus Eestis	91
5. Eesti elanike küberturvalise käitumise toetamiseks sobivate sekkumiste ja lünkade kaardistus	97
5.1. Eesti elanike küberturvalise käitumise parandamiseks sobivad sekkumised	99
6. Järeldused ja soovitused	109
Kasutatud allikad	117
Lisa 1. Meetodid ja andmed	121

Kokkuvõte ja peamised soovitused

Uuringu „Eesti elanike küberturvaline käitumine ja küberkäitumise püsiv mõjutamine“ eesmärk on aidata Riigi Infosüsteemi Ametil (RIA) paremini mõista Eesti elanike küberturvalist käitumist, selgitada välja võimalikud sekkumised, mis tulemuslikult aitavad mõjutada inimeste käitumist püsivalt küberturvalisemaks, hinnata nende sekkumiste rakendatavust Eesti kontekstis ning ühtlasi anda RIA-le praktilisi üldisemaid suuniseid, mille alusel on järgnevatel aastatel võimalik täpsemini sihitada ja ellu viia küberturvalisusalaseid ennetus- ja teavitustegevusi.

Uuringu peamised uurimisküsimused on:

- Milliseid käitumist püsivalt mõjutavaid sekkumisi on maailmas inimeste seas läbi viidud?
- Milliseid tulemuslikke küberkäitumist püsivalt mõjutavaid sekkumisi on inimeste seas läbi viidud?
- Milline on Eesti elanike küberturvaline käitumine?
- Kuidas saaks Eesti elanike küberturvalist käitumist toetada?

Analüüsist selgub, et Eesti elanike peamine ajend küberturvaliseks käitumiseks on **hirm kaotada oma raha, andmed, identiteet või privaatsus**. Eriti ettevaatlikud ollakse toimetades internetipankades ja e-poodides, kus riski tajutakse suuremana. See näitab, et **inimestel on olemas küberturvalisuse alased teadmised ja nad rakendavad neid sõltuvalt olukorrast ning motivatsioonist sageli valikuliselt ja riskipõhiselt**. Lisaks ajendavad Eesti elanikke küberturvaliselt käituma välised tegurid nagu **kohustus küberturvalisi praktikaid järgida** (nt töökohal) või **küberturvalist käitumist soosivate tehniliste/tehnoloogiliste lahenduste** (nt kaheastmeline autentimine) olemasolu. Samuti motiveerib inimesi küberturvalisusele rohkem tähelepanu pöörama **eduelamus ja tunnustus õige käitumise eest**.

Samal ajal on üks peamisi põhjuseid, miks Eesti elanikud küberruumis baashügieeni ei järgi, tingitud **uskumusest „minuga ei juhtu mitte midagi“**. Küberhaavatavat käitumist tingivad ka nt **ebaturvalised harjumused, hooletus, mugavus ja laiskus**. Peamised riskikohad inimeste küberkäitumises on seejuures nt nõrkade paroolide kasutamine ning kaheastmelise autentimise vältimine. Ühtlasi paneb inimesi, sh eriti noori küberohtusid eirama ja ebaturvalisemalt käituma ka **sotsiaalne surve ning ressursipuudus**, mille tõttu pole alati võimalik kasutada digilahendusi, mis oleksid kontrollitud ja ohutud (nt õpingute käigus vajalike materjalide ja programmide alla laadimine piraatlehtedelt).

Eesti inimesed saavad küberturvalisusalast informatsiooni eelkõige **massi- ja sotsiaalmeediast ning teistelt inimestelt** (nt pere- või sõpraderingis). Täiendavad infoallikad on **töökoht ja (kõrg)kool**, kuid koolis käsitletakse teemat mitmete intervjuueeritud noorte hinnangul kas liiga hilja, pealiskaudselt või ebahuvitavalt. Küberturvalisusalast informatsiooni leidub inimeste hinnangul piisavalt, mõnede jaoks on seda saadaval isegi

tüütult palju ja see võib vähendada võimet/tahtmist infole tähelepanu pöörata. Samas ei pruugi asjakohane info alati inimesteni jõuda ja huvi või mure korral tuleb siiski vajalikku teavet ise otsida. Ühtlasi areneb küberturvalisuse valdkond kiiresti, eeldades **teadmiste ja käitumise pidevat ajakohastamist**.

Küberturvalisusega seotud teemad, mille kohta inimesed rohkem teavet soovivad, on eelkõige tehisaru ja selle kasutamisega seonduv, (isiku)andmete kaitsmine ja privaatsus ning ka turvaliste paroolide rakendamine. Eri sihtrühmade infovajadus võib seejuures olla erinev: noored ootavad pigem süvitsiminevat ja edasijõudnutele mõeldud infot, vanemad inimesed eelistavad aga selgelt ja lihtsalt esitatud põhitõdesid.

Varasemad uuringud on küll käsitlenud nii küberturvalist käitumist mõjutavaid isiklikke ja organisatsioonitasandi tegureid ning küberturvalist käitumist edendavaid sekkumisi, ent siiski puudub teadlaste seas üksmeel selle osas, mis on inimeste küberkäitumise püsivaks parandamiseks kõige parem viis ning meile teadaolevalt pole varem süstemaatiliselt pikaajaliselt ja püsivalt just küberkäitumist mõjutavaid sekkumisi uuritud. Selle uuringu käigus koostatud **süstemaatilise kirjandusülevaate tulemusena tuvastasime kuus sekkumist, mida lühidalt kirjeldasime ja mille rakendatavust küberkäitumise edendamise kontekstis hindasime**. Nende seas **leidus kaks sekkumist, mille rakendatavust võib küberturvalisuse valdkonnas Eesti kontekstis pidada kõrgeks**: 1) individuaalselt kohandatud motiveeriv suhügieenialane programm, mis põhineb kognitiiv-käitumuslikel põhimõtetel ja motiveerival intervjuerimisel; 2) üliõpilastele suunatud neljaetapiline integreeritud küberhügieeni mudel käitumise parandamiseks.

Peamised soovitused:

Inimeste teadlikkuse ja sisemise motivatsiooni suurendamine

- Õpetada tavakasutajaid mõistma oma riskiprofiili ja võtma kasutusele kohaseid küberturvalisuse praktikaid ka väljaspool pankade ja e-poodide konteksti, kus osa inimesi juba oskab riske meeles pidada ja ära tunda. Kasutada seejuures lihtsaid, tavainimesele arusaadavaid sõnumeid, nt kampaania stiilis "Hoia, mis oluline".
- Tuletada inimestele ühtlasi järjepidevalt meelde, et kübermaailmas on kõik pidevas muutumises, mistõttu tuleb pidevalt aja ning arengutega kaasas käia.
- Jätkuvalt jagada (sotsiaal)meedias ja ka küberturvalisusalastel koolitustel reaalelulisi lugusid juhtumitest, kus kellegagi on internetis toimetades ohtusid eirates midagi halba juhtunud. Jälgida meediakajastuse puhul seejuures, et ohvritena ei kujutataks pidevalt sarnase taustaga inimesi (nt vanemaealisi, vene emakeelega inimesi, madalama haridustasemega inimesi) ning et lugude toon ja esitamisviis oleks ligipääsetav ja mõistetav kõigile eagruppidele.
- Luua mänguline küberturvalisuse test tavakasutajale, mis näitab inimese teadlikkuse taset, võrdlust teistega (keskmisega) ning annab isiklikke soovitusi küberkäitumise parandamiseks. Testi läbimise järel saab inimene individuaalsele sisendile tuginevad

soovitused ja materjalid või viited, mida ta peaks veel silmas pidama, et enda küberhügieeni parandada.

- Keskenduda küberturvalisusalase info levitamisel mitte ainult ohtudele, vaid ka küberturvalisuse positiivsele kuvandile – arukas, nutikas, atraktiivne ja väärtust loov on olla küberteadlik inimene. Uudne lähenemisenurk võib äratada ka nende inimeste tähelepanu, kellele hoiatav informatsioon on muutunud tüütavaks.
- Rakendada senisest enam küberturvalisusalast personaalset nõustamist (nt juturobotiga infoliin või veebiplatvorm; õpitoad), et iga inimene saaks vajadusel küsida just seda teavet, mis teda huvitab ja mida ta vajalikuks peab.
- Vaadata üle RIA ja partnerite kanalid ning protsessid, et leida senisest enam ja igakülgsemalt (mitte ainult tänu väljendava automaatvastusena) viise, kuidas saaks tänada/tunnustada inimesi, kes on küberohtusid märganud ja neist teada andnud. Tõsta laiemalt esile küberturvalist käitumist kui midagi tunnustust väärivat.

Sihtrühmapõhine ja kogukonnakeskne lähenemine

- Rakendada küberturvalise käitumise edendamisel kogukonnapõhist lähenemist või kõneisikuid ja kanaleid, kes/mis on teatud sihtrühmas populaarsed ja autoriteetsed ning aitavad levitada infot küberturvalise käitumise teemal.
- Vanemate inimeste küberturvalise käitumise edendamiseks kasutada kombinatsioonis nii lihtsa ja selge sisuga infovoldikud, mis tuletaksid inimestele meelde küberhügieeni põhimõtteid koos asjakohaste näidetega, kui ka personaalset nõustamist (nt üks-ühele nõustamised raamatukogudes, mida paljudes kohtades juba ka pakutakse, aga ka väikestes gruppides toimuvad õpitoad; „noorelt eakale“-juhendamine ja kogukondlike mentorite rakendamine). Tagada seejuures, et juhendajatel/mentoritel on toetava rolli tõhusaks täitmiseks ka nn tööriistakast (materjalid ja koolituspõhjad, koolitajate koolitamine, et nad teaksid, kuidas juhendada, millest rääkida jms). Võimalusel teha koostööd eagrupid populaarsete tele- või raadiosaadetega (nt „Õnne 13“, „Prillitoos“, „Päevatee“), et nende kaudu võimendada sõnumit küberturvalise käitumise olulisusest.
- Noorte suunal teha koostööd nt õpilasesinduste, noortekeskuste ja noorteühendustega ning ka noorte hulgas populaarsete brändide ja suunamudijatega. Pidada seejuures silmas, et kõneisikud oleksid usaldusväärsed, pädevad ja koolitatud teemast kõnelema ning jagaksid korrektset ja asjakohast informatsiooni.

Tõhus ja mitmekesine info edastamine

- Jätkata ka edaspidi massi- ning sotsiaalmeedias küberturvalisusalase info jagamist (sh avalike kampaaniate raames).
- Koostada konkreetseid ja lihtsaid juhiseid (nt „Kolm sammu ID-kaardi kasutamisel“, „Mida pidada silmas e-poes osteldes“, „Keda teavitada, kui saad kahtlase kõne?“ vms) vastavalt sihtrühmale ja tehnoloogiakasutusele. Eristada seejuures küberturvalisusalase info sõnumiseades ja sisulistes (juhend)materjalides rohkem telefoni ja arvutisse puutuvat, et

inimestel oleks selgem, mida ühe või teise seadme puhul silmas pidada. Levitada neid konkreetseid ja lihtsaid juhiseid mh RIA küberturvalisuse aastaraamatu avaldamise ajal, mil küberturvalisuse teema saab keskmisest enam tähelepanu ja mil on asjakohane esile tõsta ka just värskemat teavet ning aktuaalsemaid ohte.

- Kombineerida eelnimetatud tegevusi personaalsemate ja sihtrühmapõhiste lahendustega: kogukonnapõhised koolitused/mentorlus, personaalne nõustamine (nt juturobotiga infoliin või veebiplatvorm; õpitoad).

Küberkäitumise edendamine koostöös tööandjate ja õppeasutustega

- Pöörata töökohtadel rohkem tähelepanu inimeste küberturvaliste käitumisharjumuste kujundamisele, korraldades küberturvalisusalaseid koolitusi või rakendades muid asjakohaseid sekkumisi.
- Tagada tööandjatele küberturvalisusalaste koolituste korraldamiseks ja asjakohase info jagamiseks igal aastal uuendatavad kvaliteetsed sisekoolituse jm infomaterjalid (slaidiesitlused, faktilehed, nõuandeartiklid, videokoolitused vms). Koostada materjalid nii, et need on kohaldatavad sektorite/töökoha profiili/ettevõtte suuruse järgi ja vajadusel koolitada enne ka koolitajaid, kes asuvad sisekoolitusi läbi viima.
- Korraldada nii töökohtadel kui õppeasutustes ettehoiatamata toimuvaid küberõppusi või -teste, et panna inimeste teadlikkus ja valvsus reaalses maailmas proovile ning vältida võltsenesekindluse teket.
- Lõimida küberturvalisuse edendamine süsteemsemalt haridusasutuste tegevustesse läbi sisukama teemakäsitlemise ainetundides/-kursustel. Kasutada õppijates teema vastu suurema huvi äratamiseks ka haridusasutuste tegevusse lõimitavaid kollektiivseid väljakutseid, kus õpilased saavad juhendajate toel osaleda (nt küberturvalisuse teemaliste loovtööde (nt videote) konkursid / „Rakett 69“ telesaate stiilis võistlus jms).
- Koostada haridusasutuste jaoks lihtsaid ja eakohaseid küberturvalisusalaseid õppematerjale (videoloengud, tunnikavad, harjutused, (rolli)mängud jne), mida õpetajad saavad eri õppeainetes kasutada ning neist küberturvalisuse teema selgitamisel lähtuda.

Küberkäitumise edendamine koostöös teenuseomanike ja teenusepakkujatega

- Soosida selliste tehnoloogiliste lahenduse arendamist ja kasutamist, mis toetavad inimesi küberturvaliste praktikate rakendamisel, ent on samas ka kasutajasõbralikud (nt TARA kasutamine salasõnade asemel, automaatne väljalogimine jms).
- Julgustada teenusepakkujaid (nt telekommunikatsiooniettevõtteid) jagama inimestele järjepidevalt küberturvalisusalast informatsiooni. Nt lisama paberarvetele teemakohaseid infovoldikuid (eriti eakate puhul), jagama juhendmaterjale kliendivisiidi käigus jms.

Executive summary and main recommendations

The aim of the study “Cyber security behaviour of Estonian residents and permanent impact on cyber behaviour” is to help the Estonian Information System Authority (RIA) better understand the cyber security behaviour of Estonian residents, identify possible interventions that effectively support lasting changes toward more cyber-secure behaviour, assess the feasibility of such interventions in the Estonian context, and provide RIA with practical recommendations, on the basis of which it will be possible to more precisely plan and implement cyber security prevention and information activities in the following years.

The main research questions of the study are:

- What type of interventions have been implemented globally that result in lasting changes in human behaviour?
- What type of interventions have been implemented globally that result in lasting changes in human cyber security behaviour?
- What is the current state of cyber security behaviour among the Estonian population?
- How can the cyber security behaviour of Estonian residents be supported and improved?

The analysis reveals that the primary motivation for cyber-secure behaviour among Estonian residents is the **fear of losing their money, data, identity, or privacy**. People are particularly cautious when using online banking services or shopping online, because the perceived risk is higher during these activities. This shows that **individuals possess cybersecurity knowledge and apply it selectively and risk-based, depending on the situation and their motivation**. In addition to internal motivations, external factors such as **requirements to follow cyber security practices** (e.g., at the workplace) or the **availability of supportive technical/technological solutions** (e.g., two-factor authentication) also encourage secure behaviour. People are also motivated by **a sense of success or recognition for correct behaviour**.

At the same time, one of the main reasons why Estonian residents neglect basic cyber hygiene appears to be the **belief that “nothing bad will happen to me.”** Risky cyber behaviour is also influenced by **unsafe habits, carelessness, convenience, and laziness**. Key risks in people’s cyber behaviour include the use of weak passwords and the avoidance of two-factor authentication. In addition, **social pressure and lack of resources** – especially among young people – can lead to ignoring cyber threats and acting unsafely online. This includes, for instance, downloading necessary study materials (e.g., academic books/articles) and software from pirate websites due to lack of access to legitimate resources during studies.

Estonian residents primarily receive **information about cyber security from mass and social media, as well as from other people** (e.g., family or friends). Additional sources include **the workplace and educational institutions**, although several interviewed young people felt that

schools address the topic too late, too superficially, or in an unengaging way. People find that there is enough information about cyber security available – some even find it annoyingly abundant, which can reduce willingness or ability to pay attention to it. Nevertheless, relevant information does not always reach everyone, and in case of interest or concern, people often have to search for information themselves. Moreover, **the field of cyber security is developing rapidly, requiring continuous updates to both knowledge and behaviour.**

The cyber security topics that people want more information about are: artificial intelligence, protection of (personal) data and privacy, and secure password practices. Information needs vary across target groups: younger people prefer more in-depth, advanced information, while older people value clear and simply presented basics.

Although previous studies have addressed both personal and organisational-level factors influencing cyber security behaviour, as well as interventions promoting cyber security behaviour, there is still no consensus among researchers on what is the best way to permanently improve people's cyber behavior. To our knowledge, interventions that specifically affect cyber behaviour in a long term and permanently have not been systematically studied. **As a result of the systematic literature review we conducted during this study, we identified six interventions, which we briefly described and assessed for their feasibility in the context of promoting cyber security behaviour.** Among them, **two interventions were found which applicability in the field of cybersecurity in the Estonian context can be considered high:** 1) an individually tailored oral health educational programme based on cognitive-behavioral principles and motivational interviewing; 2) a four-stage integrated cyber-hygiene model for students for improving their behaviour.

Main recommendations:

Raising people's awareness and internal motivation

- Teach everyday users to understand their risk profile and adopt appropriate cyber practices beyond just e-banks or e-shops, where many people are already particularly cautious. Use simple and relatable messages, e.g., campaigns like "Protect what matters."
- Remind people regularly that the digital world is constantly changing and that they need to keep up with it.
- Continue to share real-life stories in (social) media and during trainings that show what can happen when cyber risks are ignored. Ensure that in media coverage people from similar backgrounds are not constantly portrayed as victims (e.g. older people, people with Russian as their mother tongue, people with lower levels of education) and that the tone and presentation of stories are understandable to all age groups.
- Create a gamified cyber security awareness test for everyday users, which assesses their awareness level, compares it to others, and provides personalized improvement suggestions. After completing the test, the person will receive recommendations based on

individual input and materials or references that he/she should keep in mind to improve his/her cyber hygiene.

- Promote cyber security not only through warnings but also as something smart, attractive, and value-adding. A fresh, positive image may engage those tired of fear-based messaging.
- Provide more personal cyber counseling (e.g., chatbot helplines, online platforms, workshops), so everyone can ask what's most relevant to them.
- Review RIA and partner channels/processes to improve recognition and rewarding of people who report cyber threats. Highlight and reward cyber-secure behaviour more publicly.

Target group and community-based approaches

- Use a community-based approach and spokespersons/channels popular within specific target groups to promote cyber-secure behaviour.
- For older adults: combine simple, clear informational brochures (reminding them of cyber hygiene with relevant examples) with personal counselling (e.g., one-on-one help at libraries, small group workshops, "youth-to-senior" mentoring, and community mentors). Provide mentors/trainers with a proper toolkit (training materials, guidelines, etc.). Consider partnerships with popular TV and radio shows among the elderly (e.g., "Õnne 13," "Prillitoos," "Päevatee") to amplify the message.
- For youth: collaborate with student councils, youth centers, youth organizations, and influencers/brands popular with young people. Ensure that the spokespersons are trusted, competent, trained to speak on the topic and share correct and relevant information.

Effective and diverse delivery of information

- Continue distributing cyber security information via mass and social media (including public campaigns).
- Create simple, concrete guidelines (e.g., "Three steps for using an ID card," "What to watch out for when shopping online," "Who to contact after a suspicious call?") based on target group and technology usage. Distinguish between phone vs. computer-related information to improve clarity. Disseminate these simple, concrete guideline also during RIA's annual cyber security report launch to coincide with peak public interest and to highlight fresh data and threats.
- Combine the abovementioned activities with more personalized and target-specific solutions: community-based training/mentorship, personal counselling (e.g., chatbot helpline, online platforms, workshops).

Promoting cyber-secure behaviour via employers and educational institutions

- Encourage workplaces to foster cyber-secure habits through training or other relevant interventions.

- Provide employers with annually updated, high-quality internal training materials (slides, fact sheets, articles, videos, etc.) tailored to sector, company size, and job profile. Train trainers, where necessary, before they lead internal sessions.
- Organise unannounced cyber drills/tests at workplaces and educational institutions to test people's real-time awareness and avoid false confidence.
- Integrate cyber security into (high) school curricula more systematically and engagingly. Use collective challenges to increase interest among students (e.g., creative project competitions (such as making videos) or "Rakett 69"-style cyber competitions).
- Develop simple, age-appropriate learning materials about cyber security for schools (video lectures, lesson plans, exercises, roleplays) so that teachers can use these across subjects.

Promoting cyber-secure behaviour with service owners and providers

- Support the development and use of user-friendly technological solutions that encourage cyber-secure behaviour (e.g., TARA instead of passwords, automatic logout).
- Encourage service providers (e.g., telecom companies) to consistently share information on cyber security – add brochures to paper bills (especially for seniors), sharing guiding materials during service visits, etc.

Kasutatud lühendid ja terminoloogia

ERR	Eesti Rahvusringhääling
ITL	Infotehnoloogia ja Telekommunikatsiooni Liit
PPA	Politsei- ja Piirivalveamet
RIA	Riigi Infosüsteemi Amet
VPN	virtuaalne privaatvõrk
noorem eagrupp	16–24-aastased intervjueeritavad
keskmine eagrupp	35–44-aastased intervjueeritavad
vanem eagrupp	55–64-aastased intervjueeritavad

Sissejuhatus

„Minuga seda ei juhtu.“ Eesti elanikud kipuvad küberruumis liialt usaldama oma kriitilist mõtlemist ning paljud ei usu, et nad võiksid langeda küberrünnaku ohvriks (Riigi Infosüsteemi Amet, 2025a). Just see veendumus võib teha inimesed aga hoopis küberhaavatavamaks – kui puudub tunnetus, et küberrünnak võib juhtuda ka minuga, kaob ka valvsus ja pööratakse vähem tähelepanu küberturvalisusele¹ ning seda tagavale käitumisele.

Samal ajal on mõjuga küberintsidentide² arv Eestis kasvanud. Ainuüksi 2024. aastal registreeriti pea kaks korda rohkem juhtumeid kui eelneval aastal (6515 vs 3314 mõjuga intsidenti) (Riigi Infosüsteemi Amet, 2025a). Küberruumis varitsevad ohud on seega üha levinumad ja olgugi et kõiki intsidente (nt ummistusrünnakuid) ei saa tavainimesed hoolsa küberkäitumisega ära hoida, on siiski ettevaatusabinõusid, mida igaüks saab rakendada. Vaatamata sellele, et küberohud on teada ja käitumissoovitused olemas, jätavad osa inimesi vajalikud ettevaatusabinõud aga ikkagi rakendamata.

Statistikast nähtub, et Eesti inimesi, kes pole küberruumis oma turvalisuse tagamiseks mitte midagi teinud, on vähem kui kümnendik. Ligikaudu 70% Eesti elanikest arvestab soovitusel, et salasõnad peavad olema tugevad ja üksteisest erinevad. Siiski võib inimeste küberkäitumises täheldada ka murettekitavaid suundumusi. Nt on viimaste aastate võrdluses vähenenud nende 16–24-aastaste hulk, kes muudavad sotsiaalvõrgustikes või rakendustes turvasätteid või kasutavad viirusetõrjet. (Riigi Infosüsteemi Amet, 2025a) Sellised muudatused viitavad võimalikule ohutunde hajumisele, isegi kui üldteadlikkus küberohtudest on tõusnud.

Eestis on seatud siht inimeste digipädevuse ja küberturvalise käitumise paranemisele. Nii tuuakse nt digiühiskonna arengukavas 2030 (Majandus- ja Kommunikatsiooniministeerium, 2021) välja, et enam pole niivõrd tarvis inimesi „interneti tuua“, vaid tuleb hoopis kindlustada, et neil oleksid ajakohased oskused digilahendusi praktiliselt ja ohutult kasutada. Samuti rõhutatakse kehtivas haridusvaldkonna arengukavas (Haridus- ja Teadusministeerium, 2021) vajadust arendada kõikide eagruppide digioskusi, sh digiturbepädevust, et suurendada digitaalset kaasatust. Lisaks on riigi küberturvalisuse strateegias 2024–2030 (Majandus- ja Kommunikatsiooniministeerium, 2024) üheks sihiks seatud, et Eesti elanike küberhügieeni

¹ [Euroopa Parlamendi ja Nõukogu määruse \(EL\) 2019/881](#) järgi on küberturvalisus defineeritud kui „tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest“. Küberohtu all peetakse seejuures silmas „võimalikku asjaolu, sündmust või tegevust, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada“. Siinse uuringuaruande tsitaatides võib märgata ka mõisteid nagu „internetikäitumine“ või „internetis toimetamine/tegutsemine“, mida sel juhul võib pidada samatähenduslikeks mõistega „küberkäitumine“.

² Vastavalt küberturvalisuse seadusele (RT I, 22.05.2018) on küberintsident *süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust*. Mõjuga intsidentiks loeb RIA need intsidendid, mille tõttu olid häiritud teabe või süsteemide konfidentsiaalsus, terviklus või kättesaadavus (Riigi Infosüsteemi Amet, 2023).

tase tõuseb ja väheneb nende elanike hulk, kes ei ole küberruumis oma isikliku turvalisuse või privaatsuse tagamiseks astunud mitte ühtegi sammu. Selleks, et nimetatud eesmärki täita ja et RIA-l oleks võimalik teha mõjusat küberturvalisusalast ennetus- ja teavitustööd, on aga tarvis mõista, miks on Eesti inimeste küberkäitumine selline, nagu see praegu on, ja millised tegurid seda käitumist mõjutavad ning mil moel oleks võimalik küberturvalist käitumist veelgi edendada.

Sellest tulenevalt on selle uuringu **eesmärk aidata RIA-l paremini mõista Eesti elanike³ küberturvalist käitumist, selgitada välja võimalikud sekkumised⁴, mis tulemuslikult aitavad mõjutada inimeste käitumist püsivalt küberturvalisemaks, ning hinnata nende sekkumiste rakendatavust Eesti kontekstis**. Uuringu laiem siht on ühtlasi anda RIA-le praktilisi suuniseid, mille alusel on järgnevatel aastatel võimalik täpsemini sihitada ja ellu viia küberturvalisusalaseid ennetus- ja teavitustegevusi.

Uuringu peamised uurimisküsimused on:

- Milliseid käitumist püsivalt mõjutavaid sekkumisi on maailmas inimeste seas läbi viidud?
- Milliseid tulemuslikke küberkäitumist püsivalt mõjutavaid sekkumisi on inimeste seas läbi viidud?
- Milline on Eesti elanike küberturvaline käitumine?
- Kuidas saaks Eesti elanike küberturvalist käitumist toetada?

Tegemist on kvalitatiivse uuringuga, kus andmekogumismeetoditena on kasutatud süstemaatilise kirjandusülevaate koostamist ning intervjuusid nii ekspertide kui Eesti elanikega vanuses 16–24, 35–44 ja 55–64. Täpsem info uuringus kasutatud meetoditest ja andmetest on leitav aruande lõpust (vt Lisa 1. Meetodid ja andmed).

Uringuaruanne koosneb kuuest põhiosast:

- Esimesest peatükist leiab eksperdiintervjuudele tugineva ülevaate sellest, missugused on peamised küberturvalise käitumise edendamise tegelevad osapooled Eestis, millega ja kuidas nad täpsemalt tegelevad ning mis on senise korralduse tajutud tugevused ning kitsaskohad.
- Teine peatükk keskendub Eesti elanike küberkäitumisele nii intervjueritud ekspertide kui inimeste endi vaatenurgast: kas küberturvalisus on inimestele oluline; milline on nende küberteadlikkus ja kas ning kuidas see on ajas muutunud; milliseid küberturvalisuse põhitõdesid rakendades tagavad inimesed oma turvalisuse ja kus on selles vajakajäämised; mis üldse ajendab inimesi küberturvaliselt käituma.

³ Selles uuringus on Eesti elanike all peetud silmas 16–24-, 35–44- ja 55–64-aastaseid Eesti inimesi, kes vastavalt tellija soovile moodustavad uuringu sihtrühma.

⁴ Sekkumise all peame silmas sihipärast tegevust, strateegiat või meedet, mis on suunatud üksikisikutele või rühmadele ning mille eesmärk on muuta (küber)käitumist, parandades inimeste teadlikkust, hoiakuid või harjumusi.

- Kolmas peatükk käsitleb seda, kuidas võiks Eesti elanike küberkäitumist inimeste endi ja ka intervjueritud ekspertide arvates mõjutada: kust inimesed üldse infot saavad ja kas seda on piisavalt; mis motiveeriks neid temale rohkem tähelepanu pöörama; milliseid kanaleid/formaate/sõnumeid kasutades võiks laiemas uldsuses jõuda.
- Neljas peatükk tutvustab uuringu käigus koostatud süstemaatilise kirjandusülevaate raames kogutud sekkumisi ja annab hinnangu nende rakendatavusele Eestis.
- Viiendas peatükis on süstemaatilise kirjandusülevaate ja intervjuude analüüsi tulemused esitatud sünteesitult, et tuvastada võimalikke lünki küberturvalist käitumist edendavate sekkumiste pakkumises Eestis.
- Lõpetuseks sisaldab aruanne kokkuvõtlikku osa, mis toob välja analüüsist tulenevad järeldused Eesti elanike küberteadlikkuse ja -käitumise kohta ning soovitused küberturvalise käitumise edendamiseks.

1. Küberturvalise käitumise edendamine Eestis

Enne kui keskendume Eesti elanike küberkäitumisele ja võimalikele viisidele selle mõjutamiseks, anname esmalt uuringu käigus tehtud eksperdiintervjuudele tuginedes sissejuhatava ülevaate sellest, mida eri osapooled Eestis küberturvalise käitumise edendamiseks teevad ning mis on senise korralduse tugevused ning kitsaskohad. Rõhutame, et me ei teostanud uuringu käigus süsteemset dokumendianalüüsi, hinnanud poliitikaid ega intervjuerinud poliitikakujundajaid, mis tähendab, et järgnev ülevaade on peegeldus sellest, millisena valdkonnas tegutsevad eksperdid, keda intervjuerisime, olukorda tajuvad.

1.1. Küberturvalise käitumise edendamisega seotud osapooled ja nende senine tegevus

Vastavalt RIA põhimäärusele (RT I, 28.04.2011, 1) on küberturvalisusalane ennetustöö ja avalikkuse ohtudest teavitamise korraldamine üks ameti põhiülesanne. RIA struktuuri kuulub eraldi küberturvalisuse keskus, mille analüüsi- ja ennetusosakond korraldab ja koordineeribki ennetusprogrammide läbiviimist Eestis ja inimeste küberalase riskikäitumise mõõtmist (Riigi Infosüsteemi Amet, 2025b). Samal ajal annavad oma panuse küberturvalisusalasesse ennetus- ja teavitustöösse ka teised osapooled nagu PPA, Pangaliit ja ITL ning avalikkuse või klientide harimise ja teavitamisega tegelevad ka erinevad ettevõtted. Nt on PPA ennetustöö kontseptsioonis (Politsei- ja Piirivalveamet, 2018) välja toodud, et politsei tegeleb elanikkonna teavitamisega internetis levivatest ohtudest. Pangaliidu ennetustöö fookus on eelkõige pangapettustel (Eesti Pangaliit, s.d.) ning ITL-i tegevused on esmajoonel suunatud ettevõtetele, et tõsta ettevõtjate küberturvalisusalast teadlikkust ning aidata tugevdada küberjulgeolekut laiemalt (ITL, s.d.).

Niisiis on erinevatel küberturvalisusalase ennetus- ja teavitustööga tegelevatel osapooltel oma tegevuses veidi erinev keskpunkt, kuid **nad kõik toetavad erinevate kampaaniate või muude algatuste kaudu küberteadlikkuse suurendamist sooviga mõjutada inimeste käitumist**. Kampaaniate/algatuste fookus kujuneb nii RIA kui Pangaliigu esindajate sõnul peamiselt statistika alusel (Pangaliit viib läbi kampaaniate eeluuringuid, RIA tugineb Statistikaameti andmetele) ning RIA puhul ka vastavalt levinumatele küberintsidentidele (intervjuud RIA ja Pangaliidu esindajatega). ITL-i tegevuste temaatika otsustavad liidu liikmed ehk ettevõtted, kes valivad, millisele aspektile oleks tarvis keskenduda (intervjuu ITL-i esindajaga).

Seni kasutatud ennetus- ja teavitustöö formaatidest rääkides tõi intervjueritud RIA esindaja välja nii **õpitube/koolitusi, teavituskampaaniaid, temakohaseid raadio- ja telesaateid (minisaatesari „IT-vaatlik“)**, aga ka **küberturvalisuse ennetusportaali itvaatlik.ee**. Tegevuste puhul on RIA eristanud ka eri sihtrühmi: nt seni korraldatud õpitoad on olnud suunatud

eeskätt vanemaealistele (55+) ning kunagi kasutusel olnud **küberturvalisuse infoliin** oli mõeldud vene emakeelega inimeste küberkäitumise toetamiseks. Samas infoliini puhul tõdes intervjueeritav, et seda kanalit võiks tulevikus katsetada ka laiemal elanikkonna suunal. Samuti on RIA teinud **spetsiaalselt väikese ja keskmise suurusega ettevõtetele suunatud teavituskampaaniat**, mille käigus töötati välja ka juhendmaterjale (intervjuu RIA esindajaga). Intervjueeritud ITL-i esindaja sõnul on nemad omakorda RIA poolt ettevõtete jaoks tehtud juhendmaterjale kasutanud oma ennetus- ja teavitustöös, tehes juhendeid lihtsamaks, selgemaks ja ettevõtete vaatest praktilisemaks:

RIA samal ajal [ITL-i kampaania ajal] tegi oma juhismaterjali väike-keskmisele ettevõtjale, mille pikkus vist oli mõnikümmend lehekülge. Väga selge, et üks väike-keskmine ettevõtja, kes ei tegutse IKT valdkonnas, tema juht *never ever* [mitte kunagi] ei loe seda läbi. Ja meie kuidagi proovisime viia selle [RIA poolt välja antud juhendid] kõik väga praktiliseks, palju lühemaks ja palju selgemaks – et sa ei peagi kõigega tegelema ja eelkõige sa ei pea tegelema mingisuguse IT-ga, vaid tegele oma äririskidega.

ITL-i esindaja

Kui uurisime intervjueeritud ekspertidelt (v.a RIA enda esindajalt), kuidas nad RIA poolt tehtud ennetus- ja teavitustööd hindavad, selgus, et eksperdid on selles osas kohati eri meelt. Nt intervjueeritud PPA esindaja peab RIA korraldatud kampaaniaid headeks, samas küberturvalisuse ekspert ei ole nendega rahul ja peab nende stiili küsitavaks. ITL-i esindaja hinnangul on riik küberturvalisuse teemal aga liiga vähe ära kasutanud sotsiaalmeedia pakutavaid võimalusi:

Me oleme vähe proovinud turundada küberturvet LinkedInis või Facebookis või Instagramis või kuskil sihukeses kohas – et see on sinu riigi sõnum või mingi üldtuntud sõnum sulle. Et see oleks kuidagi kohandatud, oleks kuidagi selline, et ma usun seda, see läheb mulle korda, see on kuidagi minu jaoks tehtud. Kõik see, mida sotsiaalmeedia tegelikult võimaldab.

ITL-i esindaja

ITL-i küberturvalisuse edendamisele suunatud tegevus on intervjueeritud ITL-i esindaja sõnul keskendunud praktiliste, just ettevõtete konteksti sobivate näidete/lahenduste jagamisele. Nt kasutavad nad ettevõtjate küberteadlikkuse edendamiseks **näidisjuhtumeid, mille jaoks** kaasavad kampaaniasse vabatahtlikkuse alusel mõne liidu liikmetest ja viivad läbi näitliku ründe, analüüsivad juhtumit ja koostavad selle põhjal ettevõtetele näpunäiteid.

Meie liidu liikmed on pannudki oma vabatahtliku aja, teinud nende [kampaniasse kaasatud vabatahtlike ettevõtete] tänase tehnoloogiakeskkonna kas siis sellise läbistusründe, dokumentatsioonipõhise ründe... Oleme ka päris ikkagi füüsilist rünnet proovinud realiseerida, erinevaid asju. Ja kõik see – mis juhtus; kuidas asjad olid, hästi või halvasti – selle oleme pärast kirja pannud ja oleme välja pannud ja /.../ teinudki selle kättesaadavaks liidu liikmetele. [Oleme] öelnud, et nende lühikeste põkkumiste peale, mis meil [näidisjuhtumi raames] olid, me arvame, et me liiduna võiksime õppida seda; need on need head tavad, mille järgi me [ettevõtetenä] ise peaksime käituma, et meie klientidel oleks turvalisem.

ITL-i esindaja

Lisaks on **Pangaliit 2020. aastast korraldanud iga-aastast üleriigilist reklaamikampaniat elanikkonna teadlikkuse tõstmiseks ja pangapettuste ennetamiseks** (Eesti Pangaliit, s.d.). Intervjueeritud Pangaliidu esindaja sõnul on kampaniate fookus aastate lõikes varieerunud, aga iga kord on valitud üks põhiteema, millele keskendutakse.

Intervjueeritud PPA esindaja tõdes, et **politsei tegeleb samuti järjepidevalt üldavaliku ennetus- ja teavitustööga** (nt läbi sotsiaalmeedia veebikonstaablite vahendusel), aga selle kõrval **üritab inimestele küberturvalisusest käia rääkimas ka vahetult**. Selliste kohtumiste korraldamiseks otsib PPA erinevaid võimalusi, nt pingutatakse, et teha **rohkem koostööd tööandjatega**, et nende kaudu inimesteni jõuda:

Kuna väga raske on teatud inimgruppi kuskile kokku saada, siis me oleme proovinud teha tööd selles suunas, et me teeme tööandjatega koostööd. /.../ väga palju suuri ettevõtteid Eestis on kutsunud politseinikke loengutele, kus meil on siis võimalik mitte otseselt sellele ettevõttele teha mingisugust ennetust /.../ vaid selle ettevõtte töötajatele. Me oleme nende ettevõtete juhtidele väga tänulikud, kes loovad ise selle võimaluse, kus me saame väga intiimselt minna saali ja inimestega rääkida, vestelda ja arutleda ja nende enda probleeme seal lahata. See [koolitused tööandjate kaudu] on väga hea asi – see on samm [inimestele] lähemale sotsiaalmeedia postitusest.

PPA esindaja

PPA on kasutanud ka lähenemist läbi positiivse sõnumi ehk on keskendunud avalikkuses nende inimeste tänamisele, kes ei ole pettuste õnge läinud, vaid hoopis politseid ohust teavitanud. Intervjueeritud PPA esindaja sõnul on tänusõnu edastatud raadio- ja telesinemise kaudu, lootuses, et läbi teistsuguse sõnumi saab teema rohkem tähelepanu.

Kui PPA ja Pangaliidu ennetus- ja teavitustöö on suunatud laiale üldsusele ning ITL tegeleb ettevõtjate küberturvalisusealase teadlikkuse suurendamisega, siis RIA tegevuste puhul võib sihtrühmi eristada ka kitsamalt. Intervjueeritud RIA esindaja tõdes, et eraldi keskendutakse, nagu ka eelpool välja toodud, laia avalikkuse kõrval ka ettevõtetele ning lisaks avalikule

sektorile. Lapsed ja noored on aga sihtrühm, millele RIA ei ole intervjueritud eksperdi sõnul seni eriti tähelepanu pööranud, põhjusel, et selles vallas toimetavad ka teised osapooled ning puudub ka poliitiline kokkulepe, kes selle sihtrühma küberteadlikkuse edendamisega tegelema peaks:

Eelmise aastani [2024. aastani] meie noorte ja laste sihtrühmaga eriti üldse ei tegele, sest me lootsime väga palju Lastekaitse Liidu ja "Targalt internetis" projekti peale. Aga meil oli päris suur nõudlus, et miks te ei tegele. Et miks me juba ei alusta maast madalast. Ehk siis nüüd me oleme rohkem selle sihtrühmaga ka tegelema.
RIA esindaja

1.2. Praeguse korralduse tugevused ja kitsaskohad

Lisaks seni ellu viidud tegevuste kaardistamisele uurisime intervjueritavatelt ekspertidelt ka seda, milliseid tugevusi ja kitsaskohti nad küberturvalise käitumise edendamise korralduse juures tajuvad.

Üks teema, mis vastuolulisena esile kerkis, on ennetus- ja teavitustöö **rahastamine**. Kui intervjueritud RIA esindaja sõnul on rahastuse pool (just ressursside olemasolu ja järjepidevus) olnud ameti poolt tehtava ennetus- ja teavitustöö juures praeguse korralduse üks tugevus, siis mitmed teised intervjueritud osapooled mainisid enda tegevustest rääkides pigem ressursside puudust. Nimelt saab RIA küberturvalisusalase teavitus- ja ennetustöö jaoks raha riigieelarvest, mis tähendab, et erinevalt projektipõhisest lähenemisest on olnud tagatud tegevuste süsteemsus ja jätkusuutlikkus ning rangete projektitingimuste puudumisel on võimalik katsetada uusi lähenemisi ja olla paindlikum (intervjuu RIA esindajaga). Seevastu intervjueritud küberturvalisuse ekspert nimetas ennetus- ja teavitustöö rahastamise korraldust suureks probleemiks, mis suunab valdkonnas tegutsejate energia ja ressursid raha taotlemisele ning projektkorralduslikele sammudele, mistõttu jääb vähem aega sisuliseks tööks ning ohtu satub tegevuste järjepidevus ning jätkusuutlikkus.

/.../ toetada juba olemasolevaid [algatusi], toetada pikaajalisi asju, mitte luua lihtsalt sellepärast uusi... Mitte sundida inimesi taotlema, mitte tulla kogu aeg hangetega, asjadega. Tehke toetuslepingud – teeme pika plaani. Teeme neljaks aastaks, teeme kolmeks aastaks.
küberturvalisuse ekspert

Intervjueritud Pangaliidu esindaja tõdes, et nemad rahastavad oma kampaaniat ise ning olles kampaaniat korraldades juba viiendat aastat, on juhtkond kuludega ka arvestanud. Tulevasse kampaaniasse panustavad Pangaliit ja telekommunikatsiooniettevõtted intervjueritava sõnul ühiselt. Ka ITL tagab ressursid oma küberturvalisuse edendamise

alasteks tegevusteks ise, st liidu liikmed, kes mõne kampaania korraldamisel (nt näidisjuhtumitena) osalevad, panustavad igauks ka ressursse (intervjuu ITL-i esindajaga).

PPA esindaja tunnistas samuti, et ressursipuudus on murekoht ja seda nii raha (nt professionaalse turunduse tegemiseks) kui inimeste mõttes. Arvestades, et kelmuste hulk on aja jooksul kasvanud ja politsei jaoks on ennetus küll osa tööst, ent seda tehakse kuritegevuse vastase võitluse kõrvalt ja vähese inimressursi tingimustes, oleks PPA-s tarvis oluliselt rohkem ennetustöösse panustajaid.

Intervjuude põhjal võib tõdeda, et **tehtava ennetus- ja teavitustöö mõju seiramine ning tulemuslikkuse hindamine** pole eriti süsteemne ega järjepidev. Intervjueeritud RIA esindaja sõnul toimuvad pärast ellu viidud kampaaniaid järeluuringud ning nt koolitustel osalejatelt kogutakse tagasisidet. Ka Pangaliit on oma kampaaniate järel tellinud järeluuringuid, kuid intervjueeritud isik mainis, et uuringute tulemustest väga tõsiselt ei juhinduta. PPA ja ITL oma tegevuste mõju süsteemselt ei seira (intervjuud PPA ja ITL-i esindajatega).

Kõik intervjueeritud eksperdid leidsid, et **koostöö** nende esindatud organisatsioonide **küberturvalisusalase ennetus- ja teavitustöö korraldamisel ning ellu viimisel toimib**, mitme intervjueeritava sõnul koordineeritakse omavahel eri tegevusi või sõnumeid. Nii intervjueeritud Pangaliidu, PPA kui ITL-i esindaja tõstsid eriti esile tõhusat koostööd RIA intsidentide käsitlemise osakonnaga (CERT-EE).

Me oleme väga rahul sellega, kuidas me CERT-EE-ga oleme koostöö saanud käima – infovahetuse, mis puudutab sellist kolmnurka nagu pangad, CERT-EE ja telkod.
Pangaliidu esindaja

Samas tõdesid mõned intervjueeritavad, et olgugi et omavaheline koostöö on hea, **leidub teisi osapooli, kellega koostöö seni pigem puudub, kuigi tegelikult huvi ja vajadus ühiselt tegutseda intervjueeritavate vaatest oleks**. Nt intervjueeritud PPA esindaja tõstis esile, et kohati võiks ettevõtete huvi küberturvalisuse edendamisesse panustada olla suurem. RIA vaatest oleks aga tähtis tõhustada koostööd haridus- ja noortevaldkonnaga ning seda just riiklikul, poliitikakujundajate ja rakendusasutuste tasandil, kus huvi koostööks on seni olnud pigem vähene:

See on, ma arvan, et kõige valusam punkt [koostöö haridus- ja noortevaldkonnaga]. /.../ Ja tegelikult tahakski saada... kas või Harnoga koostöö kuidagi paremaks. Sinna sihtrühma rohkem sisse saada... /.../ nii ja naa oleme proovinud. Aga ei ole see koostöö veel päriselt käima läinud.
RIA esindaja

Ühtlasi tõdes intervjueeritud ITL-i esindaja, et **see, et „RIA teab, oskab ja juhib“ on ühtaegu nii praeguse süsteemi tugevus kui nõrkus**. Üheltpoolt on tugev ja autoriteetne RIA vajalik, sest

nii on ameti sõnumid ühiskonnas usutavad. Teisalt peitub selles aga ka oht, kui üks organisatsioon on väga tugev autoriteet, ilma et oleks kõrvalautoriteeti, tasakaalu või arvestatavat konstruktiivset kritiseerijat.

Ühe kitsaskohana, mis küberturvalisusealast ennetustööd mõjutab, töid mõned intervjueritud eksperdid välja ka **seadusandluse**, mis praegu ei võimalda tõhusaimal moel avaliku ja erasektori vahel andmevahetust pidada nii (nt pangasaladuse tõttu), et intsidentidele saaks kiirelt reageerida ja küberturvalisust seeläbi suurendada (intervjuud PPA ja Pangaliidu esindajatega).

Seal [seadusandluses] on parandamise kohti küll. /.../ Pankadel ei ole õigust mingisuguse kuriteokahtluse korral politseile [sellest] teada anda – tegemist on pangasaladusega. Tahaks seda infovahetust teha paremaks, et [see] oleks selgetel juriidilistel alustel. Samamoodi infovahetus teiste osapooltega – politsei ja võib-olla ka teised pangad. Tahaks hoida üleval mingisuguseid nimekirju, kus on teada-tuntud muulakontod, mingid sellised asjad. Seda praegu teha ei saa – seadused seda ei võimalda.

Pangaliidu esindaja

Hetkel on meil seadusemuudatusega arutelud pooleli, kas on võimalik teavet erasektori ja avaliku sektori vahel paremini ja kiiremini liigutada selleks, et ka politsei saaks oma tegevusi teha reaalselt.

PPA esindaja

Suurimaks vajakajäämiseks praeguse süsteemi juures võib mõnede intervjueritud ekspertide hinnangul pidada aga seda, et **küberturvalise käitumise edendamiseks puudub koordineeritud, asutuste-/valdkondadeülene lähenemine**, seda eeskätt poliitikakujundamise tasandil. Seda murekohta rõhutasid nii intervjueritud küberturvalisuse ekspert kui ka RIA enda esindaja.

Täna ma tunnen, et rahastust ei ole. Kõik on vaesed, tehakse üksteise asju. Kogu aeg oodatakse, et keegi teine midagi teeb, ise ei tehta mitte midagi ja kui tehakse, tehakse seda sama asja, mida juba teised on teinud. Minu meelest on täiesti juhitamatu /.../, mis meil praegu toimub.

küberturvalisuse ekspert

Eriti paistab süsteemse lähenemise ja koordineerituse puudumine silma laste ja noorte küberteadlikkuse arendamise puhul, kus intervjueritud küberturvalisuse eksperdi sõnul „keskset ideed, mida hariduses teha, ei ole“ ehk puudub keskne mõtestatud lähenemine, kuidas eri osapooled ühise eesmärgi nimel võiksid sihtrühmaga tegeleda. Seda, et haridusasutustel on küberturvalisuse teemat käsitlevate materjalide ja õpetajakoolituse vastu suur huvi, tõdes ka intervjueritud RIA esindaja, tunnistades samas, et RIA on viimasel ajal

hakanud haridusvaldkonna suunal tegutsema, sest keegi teine seda lihtsalt ei tee ja vastasel juhul jäävad asjad „lihtsalt laiemat visiooni puudumise taha“.

Vahekokkuvõte

Lisaks RIA-le tegelevad ennetus- ja teavitustööga ka PPA, Pangaliit ja ITL, kes kõik toetavad erinevate kampaaniate korraldamise või muude tegevuste kaudu inimeste küberteadlikkuse suurendamist. Samuti tegelevad avalikkuse või klientide harimise ja teavitamisega ka erinevad (nt telekommunikatsiooni) ettevõtted.

RIA näeb oma teavitustegevuste sihtrühmana nii laiemat avalikkust, väikese ja keskmise suurusega ettevõtteid kui ka avalikku sektorit. Ka PPA ja Pangaliidu ennetus- ja teavitustöö on suunatud üldsusele, ITL tegeleb aga ettevõtjate küberturvalisusealase teadlikkuse suurendamisega.

Küberturvalise käitumise edendamise korralduses leidub ekspertide meelest nii tugevusi kui kitsaskohti. RIA tegevuste jätkusuutlikkus on küll seni olnud rahastuse mõttes tagatud, ent teised osapooled tajuvad enda tegevuste ellu viimisel pigem ressursipuudust. Erinevate asutuste omavaheline koostöö küberturvalisuse edendamisel on üldiselt toimiv, kuid leidub ka osapooli, kelle arvates teised võiksid teha rohkem.

Oluline murekoht küberturvalise käitumise edendamisel on osa ekspertide hinnangul ka keskse koordineerimise ja valdkondadeülese lähenemise puudumine poliitikakujundamises, mis eriti teravalt paistab silma laste ja noorte küberteadlikkuse arendamise puhul.

2. Eesti elanike küberkäitumine

Selles peatükis anname intervjuude käigus kogutud materjalile tuginedes ülevaate sellest, milline on Eesti elanike küberkäitumine: kui oluline see teema inimestele on ja kui palju nad sellele mõtlevad; kuidas nad ise oma teadlikkust hindavad; millised on nende harjumused turvalisuse tagamiseks; kus on nende teadmistes ja/või käitumises vajakajäämised ning miks nad järgivad või ei järgi küberturbe nõuandeid.

2.1. Kas küberturvalisus on inimestele oluline ja kui palju nad selle peale mõtlevad?

Valdav enamus uuringu käigus intervjueritud Eesti elanikest peab küberturvalisust oluliseks. Samas on suur varieeruvus selles, kui palju ja kui sageli inimesed küberturvalisuse peale mõtlevad – on neid, kes mõtlevad selle teema peale tihti, kuid vastupidiselt ka neid, kes tunnistavad, et ei mõtle selle peale üldse.

Inimesed, kes **peavad küberturvalisuse teemat isiklikult oluliseks, mõtlevad selle peale sageli**. Mitu intervjueritavat tõid välja, et teema on nende jaoks aktuaalne nende töö või erialase tausta tõttu: nt kuna töökohal rakendatakse turvapraktikaid või et töötatakse IT- või küberturbevaldkonnas. Teemale suunab aktiivselt mõtlema ka selle aktuaalsus ja tihe kajastus meedias ning soov end ja oma andmeid kaitsta.

See on minu jaoks oluline teema ja ma mõtlen üsna palju selle üle tegelikult. /.../
ja samas ka räägin inimestega [sel teemal] ja levitan internetiturvalisuse infot
ka mingil määral.

24-aastane intervjueritav

Ma selles mõttes mõtlen küll, et ikkagi erinevad viirusetõrjujad või see, et mida kuvatakse kasvõi tavakasutajana internetis uudiseid lugedes või kuhugi meilile sisse logides. Mis seadmest ma seda teen, kas see seade on turvaline, et uuendused oleks tehtud... Nende teemade peale ikka mõtlen regulaarselt küll.

37-aastane intervjueritav

Osa intervjueritavaid tõdes seevastu, et **kuigi nad peavad küberturvalisuse teemat oluliseks, ei mõtle nad sellele tihti ega igapäevaselt internetis toimetades**. Neile tuleb teema meelde pigem erandolukordades või kriitilistel hetkedel, kui märgatakse riski (nt kahtlasele veebilehele sattudes), või kui päriselt midagi juhtub. Mõni intervjueritav tõi välja, et tegu on iseenesestmõistetava teemaga, millele aktiivselt ei mõelda ning mis on meeles pigem alateadlikult. Intervjuudel mainiti ka seda, et teemale ei mõelda regulaarselt, kuna vajalikud seadistused on digiseadmetes tehtud ning loodetakse, et need on piisavad. Lisaks viitasid mõned intervjueritavad sellele, et nende tähelepanu on liikunud küberturvalisuselt hoopis

kitsamalt (telefoni)pettuste teemale, kuna viimane on avalikkuses enam pildis ning seetõttu eeldatavasti inimestel ka paremini meeles ja/või tajuvad nad sellega seotud riske kõrgemana.

Pigem mõtlen [küberturvalisusele] vähe. Ainult siis, kui tuleb ette see, et keegi jagab jälle mingit petukirja või et hoidke oma paroole ja muutke oma paroole järjepidevalt. Aga muidu väga mitte, et pigem just ei mõtle selle [küberturvalisuse] peale.

24-aastane intervjuueritav

Ta [internetiturvalisuse teema] on oluline, aga ta on nii iseenesestmõistetav, et kui interneti lähed, siis see ei ole nüüd küll esimene asi, mille peale mõtlen. Pigem siis, kui näed mingit saiti ja mõtled, et see ei ole nüüd see [ei ole turvaline] See hetk tekib see sulle mõttesse.

62-aastane intervjuueritav

2.2. Milline on inimeste küberteadlikkus ja kas see on aja jooksul muutunud?

Küsisime intervjueritavatelt ka, kuidas hindavad nad oma küberteadlikkust ja kas see on nende hinnangul ajas kuidagi muutunud. Ühtlasi lasime inimeste teadlikkust kommenteerida ka intervjueritud ekspertidel.

2.2.1. Inimeste küberteadlikkus ja võimekus

Üldiselt hindavad intervjueritud inimesed oma **küberteadlikkust ja võimekust internetis turvaliselt toimetada piisavaks**. Neil ei pruugi küll olla süvendatud teadmisi või arusaama tehnilistest nüanssidest, kuid nad usuvad siiski, et nad oskavad vältida levinumaid ohte. Mitmed intervjueritavad, sh IT-valdkonnas hariduse või töökogemuse omandanud inimesed, pidasid oma teadlikkust keskmisest kõrgemaks. Enda piisavat teadlikkust seostasid nad enamasti ettevaatlikkusega, nentides, et internetis toimetades järgivad nad turvalise käitumise põhitõdesid, olles lihtsalt üldiselt ettevaatlikud ja tähelepanelikud.

Mingisugused põhimõtted ma olen enda jaoks paika pannud ja teistele, kes mu ümber on, olen ka rääkinud, et teatud asju ei tehta. /.../ Ma vähemalt loodan ise, et ma enam-vähem olen oludega kursis ja natuke seda teemat jälgin ja juhtumeid ka, mis toimuvad. Ma arvan, et ma pigem tean keskmisest paremini.

61-aastane intervjuueritav

Noorema vanusegrupi esindajad põhjendasid intervjuudel enda teadlikkust lisaks ka sellega, et nad on internetiga koos nii-öelda üles kasvanud ning neile on lapsepõlvest saati küberturvalisusest räägitud.

/.../ olen teadlik internetiturvalisusest. Mulle on lapsest saati räägitud kõike seda /.../ ma tunnen, et ma tean piisavalt, et olla üpris kindel, et minu asjadele ei saa ligi. Ma arvan, et ma tean kõiki neid põhiasju, mida võiks teada.

16-aastane intervjueritav

Vaid paar intervjueritavat tunnistas, et nende **teadlikkus on madal ning nad ei ole enda võimes internetis turvaliselt toimetada täiesti kindlad.**⁵

/.../ ma ei saa öelda, et ma oleks väga sina peal kõikide turvaasjadega.

16-aastane intervjueritav

Ma ei ole endas eriti kindel /.../ ma olen nii algaja tegelikult.

58-aastane intervjueritav

Inimeste üldiselt kõrge hinnang enda teadlikkusele on kooskõlas intervjueritud küberturvalisuse eksperdi vaatega, kes peab Eesti elanike üldist teadlikkust heaks ning leiab, et inimesed oskavad küberruumis käituda.

Ma hindan seda [inimeste küberkäitumist] hindegaga 4, kui me vaatame Eestit sisemiselt. Kui me hakkame muu maailmaga võrdlema, siis ma paneksin [hindeks] 5. /.../ meie Eesti elanik on ikkagi huvitav ja õppimisvõimeline.

küberturvalisuse ekspert

Samas tõdesid nii intervjueritud küberturvalisuse ekspert kui ka ITL-i esindaja, et inimesed on erinevad ning teadlikkus ja käitumine on seega varieeruv.

Kindlasti on ta [inimeste küberkäitumine] suhteliselt hekiline. /.../ ei ole olemas keskmist eestlast. On väga servast serva – neid, kes ütlevad, et me ei julge sinna [interneti] üldse mitte midagi panna ega seal käia, see kõik on õudne; ja teised, kes seda võtavad sellise Eedeni aiana, kus midagi halba kunagi ei juhtu.

ITL-i esindaja

Meil ühiskond on ikkagi siiruviiuline. See seltskond, kellega mina suhtlen, kes on kuskil tööl või koolis või haridusega seotud, nemad on üsna hästi ära haritud.

küberturvalisuse ekspert

Kuigi enda teadlikkust turvalisest internetikäitumisest hindasid intervjueritavad üldiselt piisavaks, mainis siiski mitu inimest, et neil **on ses osas veel kindlasti arenguruumi ja nad võiksid teemast rohkem teada.** Seejuures nentisid nad, et lihtsamad ja üldteada head

⁵ Intervjuude tulemusi lugedes peab silmas pidama, et inimestel võib olla keeruline tunnistada (eriti rühmaintervjuude puhul teiste osalejate ees), et neil on puudulikud või vähesed teadmised ja oskused. Lisaks ei pruukinud uuringusse sattuda teemast vähem teadlikud või huvitatud inimesed, sest intervjuudes osalemine oli vabatahtlik ning kutse peale uuringus osaleda reageerisid tõenäolisemalt teemast ise võrdlemisi huvitatud inimesed.

praktikad on selged, kuid aktiivselt nad teemal silma peal ei hoia ning tõenäoliselt ei ole isegi teadlikud mingitest spetsiifilisematest praktikatest, mida rakendada tuleks. Ka rõhutasid intervjuueeritavad seda, et **isegi kui nad üritavad muutustega kursis olla, areneb valdkond nii kiiresti, et pole lihtsalt võimalik alati informeeritud olla ja kõike teada.**

Kuna tegemist on kogu aeg muutuva keskkonnaga, kogu aeg edasiareneva keskkonnaga, kus ohte tekib juurde, aga ka teenuseid ja muid asju ohtude vastu tekib pidevalt juurde, siis ma väga palju ei tea, sest lihtsalt ei ole võimalik nii palju seda infot tarbida ja olla alati kõige uuema infoga kursis.

19-aastane intervjuueeritav

/.../ kindlasti mul on arenguruumi. Ma arvan, et ma olen keskmine –keskmiste, levinud harjumustega /.../ ma ei hoia ise näppu peal, kas ma olen kursis kõigega või teen asju nii, nagu peab.

31-aastane intervjuueeritav⁶

Seda, et inimestel võib olla kiiresti areneva digikeskkonna ja info ülekülluse tõttu raske muutustega kaasas käia, kinnitas ka intervjuueeritud RIA esindaja, kelle sõnul on inimeste küberkäitumine aja jooksul küll paranenud, kuid samas on kindlasti veel arenguruumi, arvestades pidevalt muutuvaid ohtusid. Järelikult võib eeldada, et ka teadlikematel inimestel on keeruline end kiiresti muutuvast digimaailmas vajalike turvalisust tagavate sammudega kursis hoida.

Ma hindan, et see [inimeste käitumine küberruumis] on aastate lõikes aina paremaks läinud, aga ohte tuleb ka juurde. Kurjategijad arenevad ka. Ja kohati inimesed... nad võivad olla kursis mingite ohtudega ja teavad, kuidas teatud asju teha, aga nad ei arvesta, et uusi ohtusid tuleb nii palju peale ja nad neid ei tea. Ühesõnaga, ma arvan, et nad on tublid, aga arenemisruumi on.

RIA esindaja

2.2.2. Inimeste küberteadlikkuse ja -käitumise muutus ajas

Intervjuudest Eesti elanikega ilmneb, et valdavalt on inimeste endi hinnangul nende **teadlikkus küberturvalisest käitumisest (ja seeläbi ka küberkäitumine) aja jooksul paranenud**. Noorema eagrupi intervjuueeritavad tõid välja, et nende teadlikkus ning käitumine on paranenud seetõttu, et vanemaks saades on isiklik vastutus oma isikuandmete ja privaatsuse suhtes kasvanud ning ohud nende silmis suurenenud, sh seetõttu, et internetist on nende jaoks saanud väga oluline elu osa, mida kasutatakse üha rohkem ja isiklikult

⁶ Ühes keskmise eagrupi rühmaintervjuus osales ekslikult üks 31-aastane inimene, kuigi uuringu sihtrühma, mis oli märgitud ka intervjuu kutses, kuulusid Eesti elanikud vanuses 16–24, 35–44 ja 55–64. 31-aastase intervjuueeritava antud sisend on siiski analüüsi kaasatud, kuna sisuliselt on tegemist väärtusliku informatsiooniga ja puudub alus eeldada, et intervjuueeritava teadlikkus ja käitumine kübervaldkonnas erineksid oluliselt 35–44-aastaste vanuserühma esindajate omadest.

tähtsate toimingute jaoks. Ka vanema eagrupi intervjueeritavad tõid kasvava ohutunde välja ühe põhjusena, miks nende käitumine on aja jooksul turvalisemaks muutunud. Seejuures tõdesid erinevas vanuses intervjueeritavad, et nende ettevaatlikus on tõusnud nii küberteemade suurema esiletõusu tõttu meedias kui ka tänu kasutusse tulnud uutele digilahendustele, mis eeldavad või toetavad automaatselt turvalisemate käitumispraktikate rakendamist (nt kaheastmelise autentimise kasutamine), millega on aegamisi ära harjutud.

Ajapikku on arusaam sellest, et mis turvalisus on, kuidas seda tagada, ka paremaks läinud. Nii et seal on tulnud mingid väiksed harjumused, mis on juurde tekkinud.

19-aastane intervjueeritav

Teadlikkus ikka on tõusnud, ma arvan. Ma loodan ise vähemalt. Just tänu... kus ma nendel koolitustel olen käinud ja me peame tegema ka tööl iga aasta seda IT-testi, et seal tuleb ka selliseid toredaid asju jälle. Ma arvan, et pigem ikka tõuseb iga aastaga internetiteadlikkus.

58-aastane intervjueeritav

Mõned intervjueeritavad nentisid siiski, et nende **küberkäitumine ei ole aja jooksul muutunud ning nad on enda hinnangul kogu aeg piisavalt teadlikud olnud**. Seda mainisid kõige rohkem just vanimasse vanuserühma kuuluvad inimesed, kes tõdesid, et nad on internetis toimetades alati ettevaatlikud olnud ning üritanud teemaga kursis olla.

[Minu käitumine] ei ole muutunud, sellepärast et minu taust on ka, et ma olen õppinud programmeerimist ja töötanud IT-ettevõttes /.../ et ma võib-olla alustangi mõtteviisi sealt, ma ei mõtle enam [spetsiaalselt] sellele [küberturvalisusele].

55-aastane intervjueeritav

/.../ ma olen kogu aeg üsna ettevaatlik olnud. Võib-olla see tuleb ka vanusest, aga tegelikult olen ikka pigem ettevaatlik olnud.

59-aastane intervjueeritav

Vastupidiselt tõid aga mõned noored välja, et nende **käitumine on teatud aspektides aja jooksul muutunud hooletumaks**, kuid seejuures pole põhjus mitte puuduvad teadmised, vaid pigem mugavus.

Olen ka ise võib-olla natuke laisemaks läinud. Kui varem oli niimoodi, et ma ei kasutanud mingeid *password manageré* [paroolihaldajaid] – ma mõtlesin, et ei, ma ei anna ühele firmale kõiki oma paroole. Ja siis, kui Google küsis: "Kas ma salvestan?", ma panin "ei"... Siis üks hetk ma mõtlesin, et ah, tühja kah, niikuinii teab [Google] kõike minu kohta, olgu mul siis vähemalt mugav ja elu hea.

20-aastane intervjueeritav

Tegelikult ma arvan, et mida noorem ma olin, seda ettevaatlikum ma olin, sest siis oli see, et sulle kogu aeg ikkagi korrutatakse koolis ja igal pool [küberturvalise käitumise põhimõtteid]. Kui sa alles teed esimesi kontosid, siis ka hästi rõhutatakse seda, et peab enda identiteeti kaitsma. Aga mida rohkem neid asju tegin... Ja põhimõtteliselt ongi see, et ma ei tea, päevas korra juba lood mingi uue konto, siis enam ei mõtle selle peale nii palju ja siis see vajub ära.

22-aastane intervjuueritav

2.3. Millised on inimeste harjumused ja põhimõtted oma turvalisuse tagamiseks?

Selles alapeatükis käsitleme seda, millised on inimeste harjumused ja põhimõtted internetis toimetades ning milliste tegevuste puhul peavad nad oma turvalisust enam silmas.

2.3.1. Harjumused ja põhimõtted, mida turvalisuse nimel järgitakse

Uuringu käigus tehtud intervjuudest nähtub, et küberturvalisusga seotud harjumused ja põhimõtted, mida inimesed oma ohutuse tagamiseks järgivad, on mitmekesised.

Hoidumine kahtlasena näivatest veebilehtedest, sõnumitest ja e-kirjadest

Mitmed intervjuueritavate poolt esile toodud küberturvalisusega seotud harjumused ja põhimõtted, mida nad järgivad, seostuvad petuskeemidest ja pahavarast hoidumisega. Nt mainis valdav enamus intervjuueritavatest, et nad **ei klikki internetis toimetades tundmatutele veebilinkidele ega vasta sõnumitele või e-kirjadele, mis näivad kahtlased** (tundmatu saatja, ebaloogiline sisu, üleskutse lihtsalt lingil klikkida/sisestada oma andmed jms). Samuti väldivad inimesed enda sõnul telefonikõnesid tundmatutelt numbritelt – neid kas eiratakse või isegi blokeeritakse –, ning enne suhtlusse asumist kontrollitakse tihti, kellega on tegu (nt vaadatakse e-kirja saatja aadressi või inimese sotsiaalmeedia profiili). Seejuures töid mitmed intervjuueritavad välja, et see kõik on muutunud neile täiesti harjumuspäraseks ja automaatseks käitumismustriks. Mõned vanema vanuserühma esindajad tõdesid, et nad ei ava isegi tuttavate saadetud linke või faile, kui sõnumis puudub selgitus, millega on tegu ja miks see neile saadeti.

/.../ õnneks mul on nii kriitiline meel, et ma mingeid linke suvaliselt ei ava ja selliseid sketšisid meile ka ei ava. /.../ kui keegi võõras number mulle näiteks helistab, siis ma alati guugeldan seda. Ja kui näiteks keegi suvaline kirjutab mulle sotsmeedias, siis ma alati ei vasta, et teen seda n-ö tavainimese taustakontrolli, et kes sa oled ja miks sa kirjutad. /.../ ja mingitele sellistele, kus ma tunnen, et ah, see võib olla petukiri, siis ma juba eos ei ava, ei vasta.

24-aastane intervjuueritav

Ma ikka kõike ei ava. Hästi-hästi ettevaatlik olen ma igasuguste kirjade osas. Kontrollin näiteks alati ikkagi põhimõtteliselt, mitte 100%, aga ütleme 99%, ikkagi kontrollin ära e-maili adresseerimise, selle kes see just... et seda kontrollin. Ma tegelikult, jah, neid linke ei ava.

58-aastane intervjuueritav

Paljud intervjuueritavad mainisid ka seda, et nad reeglina **ei käi vöörastel või kahtlastel veebilehekülgedel**, eriti veebis osteldes. Üks intervjuueritav selgitas, et ta teeb enne veebipoest ostu sooritamist selgeks, kas tegu on turvalise veebilehega, guugeldades seda saiti või uurides selle kohta foorumitest, et saada kinnitust lehe usaldusväärsuse kohta. Paar intervjuueritavat märkis, et nad vaatavad veebilehtede URL-i riba, et näha, kas veebilehe aadress algab ikka HTTPS protokolliga, mis on turvalisem versioon HTTP-st.

Turvaliste paroolide ja kaheastmelise autentimise kasutamine

Teine intervjuueritav Eesti elanike poolt laialdaselt mainitud küberturvalisust tagav põhimõte, mida nad rakendavad, on turvaliste paroolide kasutamine. Intervjuueritavad tõid välja, et nad kasutavad (vähemalt teatud kontodel) unikaalseid ja tugevaid paroole. Mõned mõtleavad ise paroole välja, teised lasevad endale automaatselt paroole genereerida. Paljud intervjuueritavatest kasutavad ühte või lausa mitut paroolihaldurit. Seejuures mainisid intervjuueritavad korduvalt ka paroolide vahetamist kas sageli või aeg-ajalt. Samuti on levinud kaheastmelise autentimise kasutamine nendel kontodel, kus see on võimalik. Paar intervjuueritavat rõhutas ka seda, et nad ei jaga kunagi oma paroole või PIN-koode teiste inimestega. Smart-ID või Mobiil-ID kasutamisel koodide õigsuse kontrollimist mainis samuti paar intervjuueritavat.

/.../ [et oleks] võimalikult palju erinevates kohtades erinevad paroolid, et ei taaskasutaks paroole. Samuti see, et vahetan paroole, kui mingi aeg on möödunud /.../ Siis üks asi, mis mul on suht igal pool, kus on võimalik, et see oleks, on *two-factor authentication* [kaheastmeline autentimine].

19-aastane intervjuueritav

/.../ üritasin muuta oma paroolid keerulisemateks – eriti *Password Manageriga* [paroolihaldajaga]. Et Google ise pakub mulle paroolid välja ja siis salvestab ka, sest muidu mul ununeb kõik see ära. Ja mingid need verifikatsioonid ja asjad, et kuidagi saaks telefoniga siduda. Kui näeb, et mingi tundmatu seade üritab sisse logida [minu kontole], siis on mingi kontroll selle üle.

21-aastane intervjuueritav

Lisaks märkis osad intervjuueritavaid, et nende seadmed (telefonid ja arvutid) on paroolide või biomeetrilise isikutuvastusega (sõrmejäljelugejaga) lukustatud, et keegi kõrvaline neile ligi ei pääseks. Üks intervjuueritav tõi ka välja, et tema kodune WiFi-võrk on parooliga kaitstud.

Tarkvarauuenduste tegemine ja turvalisust lisavate lahenduste kasutamine

Tehnilise poole pealt pööravad inimesed lisaks tähelepanu tarkvarauuenduste tegemisele ja turvalisust tagava tarkvara olemasolule oma seadmetes. Intervjueeritavad tõid välja nii seda, et neil on olemas seadme enda sisse ehitatud turvatarkvara kui ka eraldi ostetud tasulise viirusetõrjeprogrammi olemasolu. Mõned intervjueeritavad mainisid ka reklaamiblokeerijate kasutamist. Kui viirusetõrjet nimetasid intervjuudel peamiselt just keskmise ja vanema vanuserühma esindajad, siis nooremad inimesed tõid enam välja reklaamiblokeerijate (nt Adblock) kasutamist. Telefonis või arvutis tarkvarauuenduste tegemist mainisid intervjuudel kõigi vanuserühmade esindajad.

.../ [olen] samme astunud, et panna hüpikakende ja reklaamide blokeerijad peale .../ Standard on küll see, et alati enne, kui ma üldse kasvõi kellegi teise arvuti sean ülesse või enda arvutit uuendan või saan uue seadme, siis ma esimese asjana tõmban alati viirusetõrjed ja muud vajalikud tarkvarad.

37-aastane intervjueeritav

.../ läpakal on ikkagi turvasüsteemid, alati uuendused ja värskendused peal. .../ Viirusetõrje – see on ka meil selline peres kõigil, et peab olema kõigil ja kõigil uued versioonid.

59-aastane intervjueeritav

Paar noorema ja keskmise vanuserühma esindajat märkisid, et pööravad tähelepanu ka **veebibrauseri turvalisusele**. Nad on teinud brauserivahetuse (nt Chrome'ist liikunud Firefoxi) ning hakanud kasutama üht kindlat brauserit, mille puhul peetakse riske väiksemaks (nt andmete salvestamise ja jälgimise poolest). Üks intervjueeritav tõi eraldi välja ka selle, et ta kustutab veebibrauseris oma sirvimise ajalugu.

Ettevaatlikkus oma andmete jagamisel ja erinevate nõusolekute andmisel

Lisaks ilmnes intervjuudest, et inimesed on **ettevaatlikud sotsiaalmeedias oma isikuandmete jagamisel**. Mitu intervjueeritavat tõi välja, et nad ei jaga sotsiaalmeedias oma isiklikku teavet (sh pilte) ning püüavad hoida enda kohta avalikult kättesaadavat infot võimalikult minimaalsena. Mõned inimesed on piiranud oma postituste nähtavust vaid sõbralistile, samas kui teised väldivad üldse millegi postitamist. Üks intervjueeritav tõi näite, et ta võtab suhtlusvõrgustikes vastu ainult nende inimeste sõbrakutseid, kelle kohta on saidil näha rohkem personaalset infot (nt nimi, vanus või pildid), mille põhjal saab teha otsuse, kas ta sõbrakutse saajat ikka isiklikult tunneb. Teine intervjueeritav täheldas, et ta ei postita sotsiaalmeedias kunagi reaajas, et vähendada turvariske – nt annab reisil olles postitamine märku kodust eemal olemisest, mis omakorda suurendab sissemurdmise ohtu.

/.../ pigem olen selline inimene, kes ei pane endast Facebooki või Instagrami või üldse sotsiaalmeediasse mingit infot üles. Et ka selline digitaalse jalajälje teema on võib-olla oluline minu jaoks.

23-aastane intervjuueritav

Profiilipildil ei ole minu nägu näha. Nimi on mul endal olemas [profiilil], sest ma ei taha, et petturid saaksid ära kasutada seda. Aga sotsiaalmeedias ei jaga infot enda kohta. Ma ei pane üles pilte endast ega ilma loata teistest inimestest, kui on privaatkonto. Avalikul kontol on väga piiratud nägemine.

39-aastane intervjuueritav

Mõned intervjuueritavad pööravad enda sõnul tähelepanu ka **nõusolekute andmisele ja veebilehete küpsistega nõustumisele**. Nad tõid välja, et püüavad vältida tarbetute nõusolekute andmist ning veebilehtedel kõigi või üldse mingite küpsistega nõustumist. Paar intervjuueritavat tõdes, et kui veebileht ei võimalda küpsiste seadeid kohandada või küpsistest loobuda, siis nad seda veebilehte ka ei kasuta. Lisaks mainis paar intervjuueritavat andmete salvestamisest hoidumist just veebis ostlemise kontekstis, rõhutades, et nad ei registreeri ennast e-poodides kliendiks ega luba makset sooritades kunagi salvestada enda pangakaardi andmeid.

/.../ püüan mitte vajutada igale poole "jah, olen nõus" suvaliselt, et näiteks küpsiste puhul püüan vältida tarbetuid nõusolekuid, kui saab ka teisiti.

42-aastane intervjuueritav

/.../ [nendele] lehtedele ei lähe välja, mis hakkavad küsima mingeid lubasid. Suhteliselt katkestan ära need. /.../ kui tahetakse mingeid küpsiseid, ma isegi sinna ei lähe tihti, kui ta ei lase mind edasi, ainult nõustumise võimalus on.

55-aastane intervjuueritav

Ettevaatlikkus digitaalse materjali alla laadimisel ja selle kasutamisel

Mõned intervjuueritavad mainisid, et nad on **ettevaatlikud faile alla laadides ja allalaetud failidega toimetades**. Nt ei lae nad alla suvalisi tundmatuid faile või kontrollivad allalaetud faile enne nende avamist, et olla kindlad, et tegu pole viirusega. Üks intervjuueritav märkis samuti, et ta vaatab nt rakenduse alla laadimisel, missuguseid nõusolekuid või millele juurdepääsu rakendus tahab ning otsustab selle põhjal, kas rakendust kasutada. Teine intervjuueritav tõi välja, et pigem ei kasuta ta enam mälu-pulkasid või kui kasutab, siis teeb enne nendelt millegi avamist või alla laadimist selgeks, kas need failid on ohutud.

.../ ma olen mod'itud [modifitseerinud] enda mingeid vanasid mängu...
Nintendo – seal on alati mingid saidid ja lingid ja asjandused, mida ma pean alla
laadima. Või kui videomängul on mingi lisaasi, siis ma alati panen selle File
Checker'isse sisse, et ta vaataks, kas seal on mingi link või midagi. .../ ma
vaatan, et see ei oleks mingi häkk.

16-aastane intervjueritav

.../ näiteks kui ma peangi mingisuguse faili avama või alla tõmbama, siis ma
ikkagi alati enne teen viirusekontrolli sellele.

37-aastane intervjueritav

Muud küberturvalisusega seotud harjumused ja põhimõtted, mida järgitakse

Eeltoodule lisaks selgus intervjuudel veel mõningaid küberturvalisusega seotud harjumusi ja põhimõtteid, mida Eesti elanikud endi sõnul järgivad. Toome järgnevalt välja mõned neist, mida üksikud intervjueritavad veel nimetasid:

- Eri seadmete kasutamine erinevate tegevuste jaoks – nt tööasjadega tegeletakse ühes arvutis ning eraasjadega teises. Üks inimene märkis lausa, et tal on eraldi arvuti selle jaoks, et teha selliseid internetiotsinguid, mida ta tavaliselt ei tee ja mille kohta ta väga palju ei tea.
- Ettevaatlikkus avalike internetivõrkude kasutamisel – paar noorema ja keskmise vanuserühma esindajat rõhutas intervjuul, et nad ei ühine ebaturvaliste WiFi-võrkudega või väldivad avalikes internetivõrkudes olulisemate toimingute tegemist. Paar intervjueritavat nentis, et nad kasutavad või on varem kasutanud virtuaalset privaativõrku (VPN-i).

.../ katsun sisse logida ainult enda võrkudesse ja arvutiga kindlasti mitte
avalikku [internetivõrku] .../ olen näiteks endale salvestanud, et ta [sülearvuti]
võtabki esimesena ainult selle võrgu, mis on turvaline ja ei lähe iseseisvalt
kusagile mujale ühenduma.

38-aastane intervjueritav

2.3.2. Teenused ja tegevused, mille puhul peetakse turvalisust rohkem silmas

Lisaks uurisime intervjuudel seda, kas leidub tegevusi või teenuseid, mille puhul inimesed eriti oma turvalisust silmas peavad ja millised need tegevused/teenused sel juhul on. Kõigis vanuserühmades kerkis esile **delikaatsete isikuandmete jagamine kui üks olulisemaid tegevusi, millega seoses inimesed rohkem turvalisusele mõtleavad**. Mõned intervjueritavad tõid välja, et nad mõtleavad turvalisuse peale siis, kui nad peavad kuskile sisestama enda nime,

isikukoodi või PIN-koode. Sellisel juhul kaaluvad nad andmete jagamist hoolikalt või teevad seda turvalisest internetivõrgust, nt kodust. Üks intervjueeritav märkis lisaks, et ta pöörab privaatsusele enam tähelepanu just pere kontekstis – ta ei jaga kunagi oma pere või laste pilte ega andmeid (sh elukohta).

/.../ kui ma kuskile pean sisestama oma isikukoodi, /.../ siis ma mõtlen ikkagist mitu korda üle. Või kui ma pean kuskile oma perekonnanime panema, siis mõtlen võib-olla mitu korda enne, kui jagan.

24-aastane intervjueeritav

/.../ kõige rohkem ma mõtlen [turvalisuse peale] siis, kui ma lähen login sisse panka või mingisse muusse digiplatvormi, eriti nende [PIN] koodide sisestamisel. /.../ digilugu või terviseteenused, maksuamet, kõik sellised, kus ma juba koodidega sisse login, /.../ seal kohal mõtlen.

58-aastane intervjueeritav

Ühtlasi tõdesid mitmed intervjueeritavad, et **panga- ja krediitkaardiandmete jagamisel ilmneb neil selge valvsus ja kõrgendatud tähelepanu ohtudele**. Intervjueeritavad tõid esile, et just internetipangas toimetades mõtlevad nad teadlikumalt oma turvalisusele. Ka e-poode kasutades ja veebimakseid tehes on inimesed keskmisest ettevaatlikumad. Nt mainisid intervjueeritavad, et nad järgivad siinkohal mitmeid küberturvalisuse põhitõdesid nagu kaardiandmete mittesalvestamine, e-poodide kliendiks mitteregistreerumine, pangast tehingute kohta teavituste saamine, pangaülekannetele makseliimitide seadmine, kasutamise järel internetipangast alati välja logimine, avalikust WiFi-st tehingute tegemise vältimine, eraldi kaardiga veebimaksete tegemine ning müüjate taustaandmete või veebilinkide kontrollimine. Rahaga seotud toimingud tõstavad järelkult inimeste jaoks tajutavat riski ning motiveerivad neid tegema küberturvalisemaid valikuid.

Panganduses [internetipanka kasutades] ma mõtlen [turvalisuse peale] veidi rohkem. Ja sotsiaalmeedias ka selles mõttes, et ma ei postita oma mingisuguseid pangakaardi paroole kuhugi /.../ pankadest ja sellistest lehtedest ma login alati end välja kohe, kui ma olen seda kasutanud.

21-aastane intervjueeritav

Just see veebis maksete tegemine – kontrollid alati üle, kas sa oled õigel leheküljel. Kui ma teen mingeid tellimusi, siis alati ikkagi need... „Turvaline e-kaubamaja“⁷ märgisega poed. Mingitelt suvalistelt lehtedelt ei telli asju. Jälgin, et see lukumärk oleks veebilehtedel olemas.

37-aastane intervjueeritav

⁷ Intervjueeritav peab ilmselt silmas E-kaubanduse Liidu kvaliteedimärgist „Turvaline ostukoht“.

Mis puudutab näiteks internetiostusid või rahaliste tehingute tegemist interneti kaudu – ma ikkagi mõtlen, kelle kaudu neid teha ja kas see müüja või rahaküsija on piisavalt turvaline ja mis andmeid ma talle annan /.../

61-aastane intervjuueritav

Mitmed intervjuueritavad (valdavalt keskmisest vanusegrupist) nentisid, et **isiklikult tähtsate kontode puhul keskenduvad nad rohkem turvalisusele kui teisejärguliste või suvaliste (nt meelelahutuslike saitide/rakenduste) kontode puhul**. Nt mainis üks noor, et kui muidu on tal igal pool kasutusel pigem üks või sarnane salasõna, siis olulisematel kontodel kasutab ta veidi tugevamaid paroole, mis sisaldavad erinevaid sümboleid. Ka keskmise vanuserühma esindajad tõid intervjuudel välja tähtsamatel kontodel tugevamate paroolide või kaheastmelise autentimise kasutamist.

Kõige olulisem turvalisus ongi meil [e-post] ise – põhimeil[iaadress] sellepärast, et sinna tuleb kõik info kokku. Kui ma sellele ligipääsu kaotaks, siis see oleks üldiselt maailma lõpp – kõik mu asjad /.../ Ma võib-olla suvalist Goodreadsi kontot ei hakka jõhkra parooliga kinni panema. See ei ole lihtsalt optimaalne. Aga Google, Instad, Messengerid, pangad, sellised asjad – need võiks siis ära turvata, et pöörata neile rohkem tähelepanu.

37-aastane intervjuueritav

/.../ kontod, millega on seotud väga palju teenuseid, näiteks Gmail või siis sotsiaalmeedia. Need peavad kindlasti olema [kaheastmelise autentimisega].

42-aastane intervjuueritav

Ka internetist millegi allalaadimine on tegevus, mille puhul turvalisust eriti silmas peetakse. Just noorema vanusegrupi esindajad, kes eelduslikult ka rohkem digitaalseid materjale kasutavad, väitsid intervjuudel, et nad pööravad sel juhul keskmisest rohkem tähelepanu turvalisusele ning kontrollivad alati allalaetavat sisu. Nt tõdesid intervjuueritavad, et nad on ettevaatlikud sellega, millistelt veebilehtedelt nad muusikat, filme, mängulisid, programme vm alla laevad. Allalaadimiseks valivad nad usaldusväärsemad veebilehed, et vältida arvutiviiruseid või muud pahavara.

Eriti kui ma laen midagi alla, siis ma alati vaatan, kas see on õige või turvaline sait. /.../ Näiteks Sims 4-s [arvutimängus] saab riideid lisada: netist leiad, et keegi on teinud iseenda disaine ja saad enda mängu lisada läbi failide. Ma alati vaatan, kas see sait on normaalne, sest väga tihti nad on kuskil tõesti x saitidel kirjas ja üles laetud ja ma ei tea, mis tuleb nendega kaasa. /.../ Ma lihtsalt vaatan lähedalt, mis programme ma laen alla. Näiteks hiljuti ma download'isin [laadisin alla] uTorrent'it. /.../ Ja siis ma panin tähele kohe, et mul on kaks veel lisa asja, mida ma ei pannud enda arvutisse. Siis ma kohe kustutasin kõik kontod, mis mul olid ja kohe kontrollisin, et mu arvuti on turvaline.

16-aastane intervjuueritav

Ühtlasi on osa intervjuueritavate sõnul nende **küberkäitumine turvalisem nt tööl või koolis, sest nende keskkondade endi sätestatud turvanõudmised eeldavad seda**. Nt töid paar intervjuueritavat välja, et nad kasutavad teatud tööasjade tegemise puhul VPN-i või ei ava võõraid e-kirju kunagi tööarvutis.

Eks ikka peamiselt ülikooliga ja tööga seotud ülesannete juures [olen eriti tähelepanelik ja mõtlen turvalisusele]. Aga ülikooliga on rohkem. Seal on hästi ranged reeglid, kuidas faile jagada, millistes keskkondades üldse infovahetus [toimub]. Seal on see [turvalisus] aktuaalsem kogu aeg. On need ülikooli ostetud litsentsid, turvalised keskkonnad.

23-aastane intervjuueritav

Muuhulgas tunnistas üks vanemasse eagruppi kuuluv intervjuueritav, et võrreldes telefoniga on ta arvutis toimetades tähelepanelikum. Ta märkis, et telefoni ekraan on väike ning klikkimise oht sinna, kuhu ei peaks, on arvutiga võrreldes kindlasti suurem, mistõttu on ta läinud teatud olulisemaid tegevusi tehes üle arvuti kasutamisele.

2.4. Kus on inimeste küberkäitumises vajakajäämised?

Olgugi et intervjuudest ilmnes, et inimesed hindavad oma küberteadlikkust pigem piisavaks ja järgivad ka erinevaid küberturvalisuse põhitõdesid, leidub nende teadmistes ja/või käitumises siiski ka vajakajäämisi. Nt mainisid mitmed intervjuueritavad **turvaliste käitumispraktikate rakendamata jätmist paroolide puhul**: ei kasutata unikaalseid ega tugevaid paroole või ei uuendata salasõnasid neid regulaarselt.

Mõned inimesed mainisid ka seda, et nad **ei kontrolli linke enne nendele klikkimist, ei kasuta VPN-i⁸, ei logi alati veebilehtedelt välja või lükkavad tarkvarauuenduste tegemist edasi.** Lisaks nentis paar intervjueeritavat, et nad **annavad digikeskkondades nõusolekuid kasutustingimusi tegelikult läbi lugemata.**

Mul on paroolidega pigem, et mul on paar parooli, millest kasutan variatsioone.

17-aastane intervjueeritav

/.../ ega ma oma pangaparoole või [üldse] paroole ka ju väga tihti ei vaheta.

58-aastane intervjueeritav

Mitu intervjueeritavat tõi välja, et nad **ei olegi teatud küberturvalise käitumise põhitõdedest teadlikud või isegi kui nad teoorias neid teavad, siis on nad ebakindlad, kuidas praktikas toimima peaks.** Küberturbepraktikate juhuslikus või ebajärjekindlas kasutamises väljendub seega teadmiste puudus või suutmatuse omandatud teadmisi rakendada.

/.../ paroolide osas ma ei ole kindel, et ma toimin õigesti.

31-aastane intervjueeritav

/.../ linkide kontrollimist... ma ei tea, kas ma teen. Ma hakkasin praegu mõtlema, kuidas teised seda teevad. Kas selleks on mingi eraldi rakendus, mis seda vahendab või mille järgi... lihtsalt vaatad oma kriitilise pilguga üle?

31-aastane intervjueeritav

Ma isegi ei teadnud, et brauseritel [turvalisuse mõttes] mingid vahed on.

37-aastane intervjueeritav

Eesti inimeste madalat teadlikkust ohtudest ning sellest, miks on vaja midagi teha, rõhutas vajakajäämisena ka intervjueeritud RIA esindaja:

Vajakajäämine on teadlikkus ohtudest, sest me näeme, kui palju meid [RIA-t] teavitatakse: kus inimesed on väga lihtlabaste petuskeemide ohvriks langenud; kus nad on jätnud ikkagi tegemata mingid lihtsad asjad – kaheastmeline autentimine, tugevad paroolid. Nad on jätnud selle äkki tegemata, sest nad ei tea nendest ohtudest. Nad ei tea, miks nad peaksid [midagi] tegema.

RIA esindaja

⁸ Tavakasutaja vaatest (erinevalt nt töökohtadest, kus ettevõtte ressursside kaitsmine on vajalik) ei ole VPN-i kasutamine tegelikult oluline, pigem tuleks jälgida, et kasutataks turvalist võrku (turvatud koduvõrk / usaldusväärne WiFi-võrk / mobiilne andmeside) ja krüpteeritud ühendust (veebiaadressi alguses on https, mitte http). See, et osa intervjueeritavatest tõid VPN-i mittekasutamist välja kui vajakajäämist oma küberkäitumises, näitab, et nad ei tea tegelikult, kas ja milleks selle kasutamine vajalik võiks olla ning kas seda nende vaatest üldse tarvis on. VPN-iga seonduvat mainisid mõned intervjueeritavad ka kui teemat, mis on neile segaseks jäänud ja mille kohta sooviksid nad rohkem infot (vt ptk 3.2.2).

Siiski kerkis intervjuudest teadmatuses enam esile see, et **teadmised on inimestel küll olemas, kuid nad lihtsalt ei rakenda neid praktikas**. Põhjuseks on sageli mugavus või riski võtmine lootusega, et midagi halba ei juhtu – inimesed saavad küll aru, et teatud käitumisviis pole turvaline, kuid valivad siiski lihtsama või kiirema lahendus. Mõni intervjuueeritav tunnistas samas ka, et ta ei teagi, miks ta pole küberturvalisuse põhitõdesid oma käitumises järginud, kuigi ta on neist teadlik.

Parooli asjades ma ei ole eriti eeskujulik. Enamasti on üks või kaks parooli, mida ma kasutan, mis ma tean, et on väga vale, aga lihtsalt nii hea lihtne on. Eriti siis, kui sa teed kasutaja, mida sa tead, et sa kasutad ainult ühe korra või kaks korda.

22-aastane intervjuueeritav

Mina ütleks, et ma kindlasti tean – ma lihtsalt ei rakenda kindlasti kõike, mida ma tean. On palju teoreetilisi teadmisi, mis kõik mind [intervjuueeritava poolt teadmiste rakendamist] ootavad.

37-aastane intervjuueeritav

Ka intervjuueeritud PPA esindaja tõdes, et inimesed ei suuda sageli enda olemasolevaid teoreetilisi teadmisi praktiliselt rakendada, sest oma käitumist ei mõtestata. Tema sõnul käituvad inimesed liiga palju justkui autopiloodil ega küsi endalt enne tegutsemist, miks midagi tehakse.

Kui me siin ka kannatanutega vestleme, väga paljud teavad seda, et igasugused kelmid ja lingid ja telefonikõned ja asjad käivad ringi. Aga selles hetkes nad ei suuda oma teadmist rakendada, sest nende mõttemustrisse või käitumismustrisse ei ole sisse ehitatud neid stoppe – “oota, miks mu käest küsitakse? Miks ma klikkan? Miks ma trükin midagi?”.

PPA esindaja

Lisaks tõi intervjuueeritud ITL-i esindaja vajakajäämisena välja, et **inimesed ei taju oma isiklikku vastutust** küberturvalises käitumises. Probleem ei seisne üksnes teadmiste puudumises, vaid ka selles, et inimesed ei mõtesta, milline on just nende endi roll digitaalsete toimingute ohutuse tagamisel.

Kõige suurem [vajakajäämine] üldistatult on isikliku vastutuse tajumine. Et kust maalt algab minu vastutus mingi teingu tegemise juures, andmete ja siis ka sellise... toimingu mõttes, et mida ma kuhu kirjutan ja mida ma kus vajutan. Et kui palju see on minu kontrolli all; palju ma peaksin olema nõudlik; mida ma peaksin aktsepteerima; seesama oma õiguste teadmine ja oma õiguste kaitse, et ma aktiivselt tegelen sellega, et midagi, mida ei peaks juhtuma, ei juhtuks, ja ma saan aru, et ohh, siin minnakse mingist piirist üle, või...

ITL-i esindaja

2.5. Mis ajendab inimesi küberturvaliselt käituma – või mitte?

Selles alapeatükis käsitleme seda, mis paneb inimesi küberturvaliselt käituma või vastupidi – miks küberturbe nõuandeid ei rakendata.

2.5.1. Ajendid küberturvaliseks käitumiseks

Esmalt anname ülevaate sellest, mis paneb inimesi küberturvalisusele mõtlema ja turvaliselt käituma.

Hirm kaotada raha/andmed/identiteet/privaatsus

Uuringu käigus tehtud intervjuude põhjal võib öelda, et Eesti elanike peamine ajend küberturvaliseks käitumiseks on ohtude tajumine ja arusaam, mis võib juhtuda, kui küberturbe nõuandeid ei järgita. Meedias on palju juttu erinevatest petuskeemidest, mis päädivad inimeste jaoks nt oma rahast ilma jäämisega, ning ka mitmed intervjuueeritavad töid vesteldes välja, et **hirm sattuda pettuse ohvriks ja kaotada raha**, on miski, mis ajendab neid küberturvalisuse peale mõtlema ja oma käitumist silmas pidama.

./.../ et oma rahast mitte ilma jääda ja oma isikust mitte ilma jääda, siis sellele [küberturvalisusele] peab üha rohkem ja rohkem ja rohkem rõhku panema. Ma arvan, et isegi kui su isikuandmed varastatakse, siis lõppeesmärk on sellel ikkagi kas sult otseselt raha varastada või sinu isikuandmete abil kiirlaenu või midagi taolist võtta.

38-aastane intervjuueeritav

Rohkem mainisid intervjuudel hirmu raha kaotamise ees just keskmise (35–44) ja vanema (55–64) vanuserühma esindajad, noored tõstsid esile aga pigem muid ajendeid (vt edasi allpool). Võimalik, et seda võib seletada ka sellega, et noorte puhul on summad, mida kaotada on, ka lihtsalt väiksemad. Seda tõdes ka üks intervjuueeritud noortest, kes mainis raha kaotamist küll hullimana, mis võib juhtuda, kui küberturbe nõuandeid ei järgi, ent tõdes samas, et palju kaotada poleks:

Kui keegi kuidagi rööviks mu raha ära, see oleks väga jube. Mitte et mul seda väga palju oleks, aga lihtsalt.
17-aastane intervjuueritav

Enim põhjendasid intervjuueritavad küberturvalisust tagavate ettevaatusabinõude rakendamist aga sellega, et neile **on väga tähtis kaitsta oma andmeid (nt isikuandmeid, aga ka fotosid), kontosid ning identiteeti**. Seda, et andmete lekkimisega kaasnevad lisaks võimalusele kaotada raha ka muud ohud, teadvustavad erinevas eas inimesed, tuues välja nii võimalust sattuda survekamise või identiteedivarguse ohvriks, aga ka seda, et kui inimesel juba kord on digitaalne jalajälg, tuleb oma andmete eest ka vastutada:

Ma olen näiteks kuulnud ja vaadanud dokumentaale juhtumite kohta välismaal, kus on /.../ tehtud tööpakumine läbi mingi suhtluskanali /.../ on olnud link näiteks kohtumisele või millelegi, mis tundub normaalne peale mingit lühikest vestlust. Ja siis tänu sellele on saanud kätte isikuandmed ja on hakatud inimest ähvardama päris elus. Minu arust see võib-olla hullem [...], kui asi valgub sinu elusse väljaspool interneti. Ja see on ka veidi, miks tuleb olla [internetis tegutsedes] ettevaatlik, et seda ei juhtuks.
19-aastane intervjuueritav

Peamine [hirm] ongi see, et ma kaotan ligipääsu enda kontodele ja andmetele ja keegi võib minuna esineda.
39-aastane intervjuueritav

/.../ sinu tegevustest jäävad jäljed maha ja sa ei taha ometi, et need asjad kuhugi hulkuma lähevad või sinu andmed lähevad hulkuma. Ma ei tea, sa oma asju ju hoiad, samamoodi pead ju oma andmeid [internetis] ka hoidma.
59-aastane intervjuueritav

Sageli on andmetel, eeskätt fotodel ka emotsionaalne väärtus, mistõttu peavad inimesed oluliseks end küberohtude eest kaitsta:

Meil oleks väga kahju, kui meie kogutud andmed läheksid [kaduma], me ei saaks neid taastada. Ikka aastate jooksul on sinna igasugust isiklikku infot kogunenud. Ja me oleme harjunud tegelikult pilte ja selliseid asju kusagil pilves hoidma. Ei tahaks väga, et keegi sinna ligi pääseb ja selle konto näiteks ligipääsmatuks muudab minu jaoks. /.../ E-maili kontode asjad on tõesti aegade algusest saadik siin, rohkem kui 20 aastat juba osadel inimestel ja seal tõesti on kõik. Kõik kontaktid on seal. See on täpselt nagu telefoniraamatki, et kui see ära kaob, siis on maailm korraks täitsa sassis.
59-aastane intervjuueritav

/.../ mul ei ole Google Drive'i fotod näiteks back-up'itud [varundatud], et kui keegi läheks, saaks ligi minu fotodele ja... /.../ kuidagi ma kaotaksin näiteks üle 10 aasta mingisuguseid mälestusi. Ma ei tea, võib-olla see on hullem kui see, et keegi mu pangakontolt 1000 eurot ära võtab.

39-aastane intervjuueritav

Samas oli ka intervjuueritavaid, kes tõdesid, et isikuandmete lekkimist nad ei pelga või et identiteedivargust kui üht võimalikku riski ei ole nad endale eriti teadvustanud.

Lisaks rõhutasid eriti just noorima vanusegrupi (16–24-aastased) intervjuueritavad, et küberturvalise käitumise ajendiks on **soov kaitsta oma privaatsust, sh ka füüsilist turvalisust**. See, et ligi pääsetaks nende kontodele ja seal leiduva põhjal saaks tuvastada isiku harjumusi, eelistusi jms tundub mitmete noorte jaoks hirmutav, mistõttu panustatakse oma seadmete ja kontode turvalisuse tagamisse. Osa noori tõi välja, et nad ei jaga internetiavarustes oma elukohaandmeid või pilte, mis võimaldaks liiga täpselt tuvastada pildil olija(te) asukohta. Samuti mainis üks 17-aastane intervjuueritav, et ta ei seo omavahel erinevaid sotsiaalmeedia kontosid, sest tema hinnangul võib see muuta ta kergemini leitavaks ja tema tegemised võõrastele hõlpsamini jälgitavaks, mida ta aga ei soovi.

Kohustus järgida küberturvalisi praktikaid

Eeltoodu kõrval on üks küberturvalise käitumise ajend ka **kohustus teatud praktikaid järgida**. Nimelt tõdesid mitmed keskmise eagrupi ning ka üks vanema vanuserühma esindajatest intervjuul, et nad järgivad küberturvalise käitumise põhitõdesid, kuna nii on töökohal ette nähtud. Seejuures võib kohustusest saada harjumus, mis kandub edasi ka töövälisesse konteksti.

/.../ oma töö tõttu ma pean sellele [küberturvalisusele] igapäevaselt mõtlema. Ja tänu sellele siis ka sellised [küberturvalised] käitumuslikud mallid on koju edasi kandunud.

38-aastane intervjuueritav

Toetavad tehnilised/tehnoloogilised lahendused

Ühtlasi selgus intervjuudest, et **inimesi ajendab küberturvaliselt käituma see, kui tehnilised lahendused (nt teatud kohustuslikud sätted, automaatsed hoiatused/meeldetuletused) nügivad neid ohutusele tähelepanu pöörama**. Seda tunnistasid mitmed intervjuueritavad eeskätt seoses paroolidega – kuna paljud veebisaidid nõuavad tugevate paroolide kasutamist ja on tekkinud ka rohkem kasutajasõbralikke võimalusi oma paroolide haldamiseks, siis on intervjuueritavad endi sõnul võtnudki kasutusse turvalisemad salasõnad. Sama tõdes üks intervjuueritud noortest ka kaheastmelise autentimise puhul:

Selles suhtes [käitun] turvalisemalt küll, et nüüd on üsna kohustuslik see, et sul peab olema igal pool kaheastmeline tuvastus. /.../ varasemalt ma ei kasutanud seda üldse.

24-aastane intervjuueritav

Samuti tõid intervjuueritavad paaril juhul välja, et on mugav, kui paroolihaldur teavitab neid sellest, et mõni nende salasõnadest on osalenud andmelekkes. Nii ajendab vastav teavitus paroole muutma ja seeläbi oma turvalisust tagama.

Tegelikult iPhone'il on rakendus, mis haldab paroole ja siis aeg-ajalt saadab ka... Just hiljuti saatis mingisuguse märkuse, et on mingid paroolid, mis on kuskil läinud lendama [lekkinud]. Veel ei ole jõudnud [neid paroole muuta], aga mul on kirjas see.

42-aastane intervjuueritav

2.5.2. Ajendid küberhaavatavaks käitumiseks

Lisaks uurisime intervjuudel seda, miks küberturvalist käitumist ei rakendata. Intervjuueritavad said selgitada nii seda, miks nad ise kipuvad mõnikord turvalisi käitumispraktikaid eirama, kui seda, miks inimesed üldiselt nende meelest alati küberturvaliselt ei käitu. Selgus, et ajendeid küberhaavatavaks käitumiseks on palju ja eriilmelisi.

Ohutaju puudumine naiivsusest või uskumuse tõttu, et „minuga ei juhtu midagi“

Intervjuudest ilmnas, et üks peamisi põhjuseid, miks küberturbe nõuandeid ei järgita, on inimeste arvates naiivsus või uskumus, et nemad ei satu internetis toimetades ohtu. Paaril korral mainisid intervjuueritavad, et leidub inimesi, kes on liiga heausklikud, võtavad kõike tõe pähe ja on ülemäära usaldavad, mistõttu langetaksegi pettuste ohvriks.

Paljud intervjuueritavad tunnistasid ka seda, et levinud on uskumus, et küberohtude küüsi langevad mingid ebamäärased „teised“, kes on vähem teadlikud, rumalamad ja ei mõista ohtusid.

/.../ ja siis on seal [teiste inimeste kogemuslugude] kõrval need inimesed, kes ütlevad, „Ha-ha-ha, minuga küll niimoodi ei juhtu. Vaata, kui rumal ta oli.“ Aga need on need inimesed, kellega see järgmisena juhtub.

39-aastane intervjuueritav

Seejuures tõdesid mõned intervjuueritavad, et valvsust uinutab see, kui midagi veidigi hirmutavat pole endal pikka aega kübersfääris juhtunud ja nii arvatakse, et ollaksegi väljaspool ohtu:

Võib-olla mõni inimene lihtsalt... ta arvab, et kui ei ole juhtunud, siis ei juhtu ka mitte kunagi. Võtab kuidagi lihtsamalt seda teemat. /.../ Ja et see [ohvriks langemine] on üks, ma ei tea, mitme seas.

17-aastane intervjueritav

On märgiline, et nii mõnedki intervjueritavad tunnistasid, et nad ei pööra küberturvalisusele nii palju tähelepanu, kui peaks, kuna nende riskitaju pärsib tunne, et nad on tavalised inimesed, nende andmed või kontod ei ole seetõttu nt häkkeritele atraktiivsed ja seega on nad justkui väljaspool ohtu. Mitmel korral peegeldasid seda arusaama just nooremad intervjueritavad, kes leiavad, et neil pole (veel) midagi väga olulist kaotada. Samas tõdes üks neist seejuures, et tegelikult saab ta aru, et iga tavaline inimene võib samuti ohvriks langeda.

Võib-olla mul sellepärast ongi veidi väiksem see hirm [ohvriks sattuda], et ma ise tunnen, et mul ei ole väga midagi veel varjata, kuna ma alles alustan iseseisvat elu.

22-aastane intervjueritav

Ma tean, et see võib-olla ei ole hea, aga /.../ mul on natuke suva. /.../ Ma ei tunne, nagu mu informatsioon oleks nii tähtis. /.../ Väga paljud inimesed lihtsalt ei arva, et neilt on väga midagi varastada, mis on natuke minu mõtlemine ka... mul otseselt ei olegi. /.../ Inimesed lihtsalt ei arva, et neilt on midagi väärt võtta, sest lihtsalt on nii palju inimesi internetis. /.../ Aga tavalisi inimesi just vaadatakse kõige rohkem.

16-aastane intervjueritav

Seda, kuidas inimesed kipuvad arvama, et asjad juhtuvad kellegi teise, aga mitte nende endiga, ilmestab kohati hästi ka see, kuidas eri vanuserühmadest intervjueritavad end selles uuringus väljendasid. Mitmed intervjuudel osalenud nooremast vanuserühmast rõhutasid, et nende meelest satuvad nt pettuste ohvriks või jäävad oma andmetest ilma pigem vanemad inimesed, sest nad on vähem ohtudest teadlikud ja/või naiivsemad. Samal ajal tõstsid aga nii mõnedki vanema vanuserühma esindajad intervjuudel esile, et hoopis noored on need, kes käituvad internetis hooletult ega võta ohte tõsiselt.

Isegi võib-olla nooremad [inimesed] on rohkem [küberohtudest] teadlikud... mitte siis seda, et vanemad inimesed ei ole, aga ma näen, et nad on rohkem naiivsemad kuidagi. Nad lähevad rohkem sellega kaasa, isegi kui sellest [küberturvalisusest] on räägitud.

16-aastane intervjueritav

Noored võib-olla oma hullusest, tähelepanematuses – kuna nad on enda arvates väga vanad kalad juba internetis – nad ei oska ohtu tõsiseks pidada.

62-aastane intervjuueeritav

Seda, et inimesed ei usu, et just nemad võivad internetis toimetades ohtu sattuda, olgugi et nt petuskeemid on loodud väga erineva taustaga inimeste mõjutamiseks, tões ka intervjuueeritud PPA esindaja. Ühtlasi viitas ta, et siinkohal võib inimeste ohutajule karuteene teha ka meedia, kuna pettusi kajastades küsib ajakirjandus politseilt sageli, millise profiiliga kannatanud on ehk „kuidagi tahetakse fookus tõmmata ära selle pealt, et see ei ole mina või minu partner või minu töötaja“ (intervjuu PPA esindajaga).

Mugavus ja laiskus pärsib küberturvalist käitumist

Väga sageli mainisid intervjuueeritavad seda, et küberturvalise käitumise praktikaid ei rakendata (kas üleüldiselt või konkreetselt nemad ise), kuna niimoodi on mugavam ja/või pole lihtsalt viitsimist olulisi küberturbe põhitõdesid järgida. Nt tões üks 18-aastane intervjuueeritav, et kui tema kontosid häkitaks, siis ei juhtuks see mitte sellepärast, et ta polnuks turvanõuetest piisavalt teadlik, vaid seetõttu, et ta ei viitsinud kas laiskusest või lohakusest neid nõudeid rakendada.

Eriti tõstsid intervjuueeritavad kasutajamugavuse vs turvalise käitumise dilemma esile paroolide ning kaheastmelise autentimise puhul, kusjuures seda kõigi intervjuudesse kaasatud eagruppide esindajate seas. Seda, et just turvaliste paroolide kasutamine on inimeste küberkäitumises üks peamisi vajakajäämisi, tõime välja ka juba eelpool peatükis 2.4, kus ilmnes samuti, et küberturvalise käitumise prioriteediks seadmise puhul on takistus sageli mugavus/viitsimatus, mitte teadmiste puudumises. Uurides intervjuueeritavatelt, miks nad küberturbepraktikaid järgivad või ei järgi, selgus ka siinkohal, et leidub nii neid inimesi, kes küll kasutavad kaheastmelist autentimist, kuid seda vaid siis, kui see on teatud rakenduse/teenuse puhul kohustuslik või kui tegu on olulisemate kontodega, aga ka neid, kes ebamugavuse tõttu praktikat ei rakendagi.

/.../ kohtadel, kus ei ole seda [kohustuslikku kaheastmelist autentimist] vaja, siis ma ikkagi pigem ei kasuta. Lihtsalt sellepärast, et see on tegelikult ebamugav ja võtab aega. /.../ Ja see paroolide vahetamine ka /.../ see on nii ebameeldiv.

24-aastane intervjuueeritav

Mul on kaheastmeline autentimine osades kohtades, mis mõnikord ajab mind närvi, sest näiteks ma tahaks mõnikord telefoni koju jätta, kui ma olen otsustanud, et ma ei vaja sellel päeval telefoni, aga siis nagu jõuan kuskile ja pean /.../ telefoni kaudu ennast tuvastama. Aga mul on sellistes põhikohtades see [kaheastmeline autentimine] olemas.

31-aastane intervjuueeritav

Kaheastmelise autentimise puhul tunnistan tõesti üles, et ei kasuta, sest vastus on: tüütu. Sa tahad midagi ruttu ja siis hakkab pihta /.../ See on lõivu maksmine mugavusele. /.../ Ma juba annan ka endale täiesti aru, et kaheastmeline autentimine oleks tegelikult vajalik /.../ aga jah, ma ei kasuta seda.

62-aastane intervjueeritav

Üks intervjueeritav tunnistas ka, et kuna ta on väga aktiivne interneti kasutaja, siis olgugi et ta teab, kuidas oleks turvalisim viis toimida, valib ta lõpuks teatud juhtudel ikkagi mugavama lahenduse, kuna asju, mida on tarvis teha / kuhu sisse logida, on lihtsalt hulgaliselt. Nt tõi ta välja, et ta kasutab ühte ülimalt turvalist brauserit, aga selle kõrval ka Firefoxi, ning kuna turvaline brauser ei võimalda küpsiseid ja tal tuleb seetõttu igale veebilehele iga kord uuesti sisse logida, siis ta seni lõplikult ja täielikult mugavuse tõttu turvalise brauseri kasutamisele ümber lülitunud pole.

Siinkohal on oluline rõhutada, et olgugi et intervjueeritavad esitlesid neid näiteid kui kasutajamugavuse vs turvalise käitumise dilemmat, ei tohiks see ideaalis olla valik ühe või teise kasuks, vaid pigem tasakaal, kus turvalised ja korrektset küberkäitumist toetavad lahendused on ühtlasi kasutajasõbralikud ja mugavad rakendada.

Mugavuse ja laiskusega seostub ka vastumeelsus küberturvalise käitumise vastu oludes, kus inimesel pole asjakohaseid teadmisi või teema vastu huvi ja seega on vanaviisi jätkamine mugavam. Sellist ajendit ilmnes intervjuudest just vanema eagrupi esindajate puhul.

/.../ kõigil on täiesti oma elu, eks. Oma huvid. Ja siis tüütu on ettevaatlik olla või mõelda tehniliselt sellest.

55-aastane intervjueeritav

Ka tõdes üks 58-aastane intervjueeritav, et tal küll on, kelle käest vajadusel IT-alast nõu küsida, kuid selleks on tarvis julgust, aega ja tahtmist, et küsimusi esitada, mistõttu „mugavam on toimetada nii edasi, nagu ma toimetan“.

Hooletus/väsimus/kiirustamine tingib küberhaavatava käitumise

Lisaks kartmatusele, mugavusele ja laiskusele mängivad küberturvaliste praktikate rakendamata jätmises olulist rolli ka hooletus, väsimus ja kiirustamine. Uurides, miks inimesed alati küberturbe nõuandeid ei järgi, tõstsid intervjuudel just seda põhjust rohkem esile noorema ja vanema vanuserühma esindajad. Seda mainisid ka keskmise eagrupi intervjueeritavad, ent vähem.

Mitmel korral kerkis esile kiirustamine, mis tingib selle, et turvalisus jääb tahaplaanile. Nt üks intervjueeritud noor tõdes, et eriti kipub ta kiirustama ja küberturbe põhitõdede järgimist unustama, kui ta kasutab digivahendina telefoni. Üks 58-aastane intervjueeritav tunnistas aga, et temal võib jääda midagi olulist märkamata, kui uusi e-kirju on palju, ta loeb neid kiiresti ja ei pane seega võib-olla piisavalt ohtusid tähele.

Lisaks kiirustamisele on riskantsed olukorrad, kus mängus on väsimus või emotsioonid. Üks 24-aastane intervjueeritav mainis, kuidas ta on endale seadnud reegli, et kui on tarvis e-poest midagi osta või tegeleda mõne eriti olulise kirjaga, siis ei tegele ta nende asjadega kunagi hilisõhtul väsinuna või kiirel hetkel, kui tähelepanu on hajunud. Seda, et väsimus ja emotsioonid mängivad hooletusvigade tekkimisel märkimisväärset rolli, tõdesid intervjuudel ka vanema vanuserühma esindajad:

Mingil hetkel võib-olla tähelepanu hajub või sa oledki juba liiga kaua aega internetis olnud. Enda puhul võin öelda, et see oli ikkagi enamasti tähelepanematuses [et ei olnud hoolas].

59-aastane intervjueeritav

Mõnikord tulevad lihtsalt lohakusvead. Või ma olen liiga endast väljas, et üldse midagi jälgida.

59-aastane intervjueeritav

Üks intervjueeritud noor tunnistas ka, et ohutaju võib kaduda nt interneti vahendusel asju müües, kuna rõõm sellest, et millelegi leidub ostja, paneb riske unustama:

Just selle kindla juhtumiga [Facebook Marketplace'i petturid] ja kui sarnased olukorrad on olnud, et siis on see, et lihtsalt adrenaliin on sees, et "oh, keegi tahab osta seda kleiti". Ja siis isegi ei mõtle sellele, et seal võiks olla halb inimene taga või üldse arvuti taga. Et võib-olla isegi seda kõige rohkem, et lihtsalt tuhin on sees ja kõik tundub nii õige. Ja siis ei ole nii õige.

22-aastane intervjueeritav

Seda, et küberhaavatavat käitumist võib tekitada väsimus, mis paneb inimesi tegutsema hooletult ja justkui autopiloodil, rõhutas ka intervjueeritud ITL-i esindaja:

Kriitiline koht ongi seal, et kui kogu aeg vajutada, vajutada, vajutada [peab silmas nt küpsiste (mitte)aktsepteerimist, kasutajatingimustega nõustumist jms], siis väga-väga keeruline on, kus see vajutamine ei tohiks olla nii automaatne. Ma olen seda korduvalt nimetanud ka kognitiivseks ülekoormuseks ja sellega toimetulekuks. Otsuste hulgad, mis inimesel on internetis käitumisel, on nii suured, et otsuste maht on selline, et ta on kella 10ks hommikul juba väsinud ja kogu ülejäänud päeva ta on automaat.

ITL-i esindaja

Küberturvalisusalased teadmised on puudulikud, ülehinnatud või praktikas rakendamata

Seda, et teadmiste puudumine või nende praktikas rakendamata jätmine, on Eesti elanike küberkäitumises üks peamisi vajakajäämisi, tõime välja ka eelpool peatükis 2.4. Uurides intervjueeritavatelt, miks nad ise kipuvad mõnikord turvalisi käitumispraktikaid eirama või

mis põhjustel inimesed üldiselt nende meelest alati küberturvaliselt ei käitu, kerkis ka siinkohal esile teadmiste ja teadlikkusega seonduv.

Korduvalt mainisid intervjueeritavad, et nad arvavad, et küberturvaliselt ei käituta, sest kübermaailm tundub keeruline ja inimesed ei saa sellest temast lihtsalt aru ehk puuduvad vajalikud teadmised. Samas on märgiline, et teadmiste puudumisest räägiti peaaegu alati selles võtmes, et teadmised puuduvad teistel, aga ennast niivõrd kriitiliselt ei hinnatud. Eelkõige rõhutasid intervjueeritavad (kusjuures, eri vanuses intervjueeritavad) teadmiste puudumist ühe küberhaavatava käitumise põhjusena just eakamate inimeste näitel, mis aga ei tähenda, et eakamatel inimestel kindlasti küberturvalisusalased teadmised puuduksid, vaid et teised inimesed omistavad neile madalamat digipädevust.

.../ vanemad inimesed näiteks võib-olla ei tea isegi .../ mis need ohud võivad olla. Ja kindlasti ka lapsed.
21-aastane intervjueeritav

.../ mulle tundub, et see väga suur erinevus tuleb ealiselt. On ikkagi teatud põlvkonnast alates, kes võib-olla seda asja [küberturvalisusega seonduvat] nii hästi ei jaga suures osas ja nad ei oska tunnetada ohtu.
37-aastane intervjueeritav

Ma arvan, et just vanemate inimeste puhul on see, et nad ei oska neid ohte näha .../ nad ei saa aru, et see on oht. .../ Teadlikkus on nii madal.
58-aastane intervjueeritav

Üks 23-aastane intervjueeritav tõdes, et kui tema teaks küberohtudest rohkem, siis usutavasti see paneks teda oma turvalisusele rohkem mõtlema ja seeläbi ka küberturvalisemalt käituma.

Lisaks teadmiste puudumisele mainisid intervjueeritavad paaril korral, et küberhaavatavalt käituma võib ajendada ka oma teadmiste ülehindamine ja sellest tulenev liigne enesekindlus.

Mõnel juhul tõusis intervjuudes esile ka see, et info küberturvalistest käitumispraktikatest võib küll inimesteni jõuda ja teadmised on seega justkui olemas, ent praktikas neid ei rakendata. Eelkõige nooremad intervjueeritavad leidsid, et üks võimalik põhjus, miks selline olukord tekib, on küberturbealase info üleküllus, mis viib selleni, et enam ei saada aru, mida oleks ikkagi õige teha. Infot ja teadmist on liiga palju, mistõttu loobutakse valikute tegemisest ega võeta üldse midagi ette.

Kogu aeg reklaamitakse YouTube'is näiteks mingeid VPN-e või .../ Mina ei saa aru, missugune teenus on kõige parem. Ma ei tea, mis kõik kaasneb sellega. Sest neid on nii palju, neid turvalisusteenuseid. Igal pool kogu aeg müüakse kellelegi midagi. .../ See on alati väga segadust tekitav, kui mulle proovitakse müüa midagi ja ma: "Aga mis nagu erinevus on? Kas kõik ei teegi niimoodi?"
16-aastane intervjueeritav

Väga palju valikuid väsitab inimese ära. See on ka kahjuks suur /.../ põhjus, miks inimesed lihtsalt annavadki väga kergelt üles oma selle isiksuse siis, oma andmed. /.../ Raskem on öelda „ei“ ja võidelda, sest siis sa pead vaatama [tingimusi] ja valima. Ja see on jälle lisavalik sinu elus, kus sul vahepeal niigi on tihtipeale valikuid vaja teha. /.../ pigem ma mõtlen või kulutan oma energiat selle peale, mis mul homme plaanis on, mis ma süüa teen, kui selle peale, et oota, kas ma nüüd annan neid andmeid kuhugile; kas see on nii oluline? Ja paljud otsustavad, et see ei olegi oluline.

24-aastane intervjueritav

Üks intervjueritav tõi ka välja, et kui küberturvalisusest on palju juttu ja infot on rohkelt, võib inimestel tekkida ka ärevus, et äkki käitutakse hoopis valesti; veel leidub mitu asja, mida tuleks lisaks teha, et kõik oleks korrektne jne. See omakorda võib viia selleni, et ärevuse tõttu ei tahetagi küberturvalisusega tegeleda ning muututakse seetõttu haavatavaks.

Küberturvalist käitumist takistab sotsiaalne surve

Üks teema, mis tõusetus mõnel korral noorema ja keskmise eagrupi esindajaid intervjuerides, on sotsiaalne surve, mis paneb küberohtusid eirama ja käituma ebaturvalisemalt, kui muidu ehk inimesele omane oleks. Nt tõi üks intervjueritav välja, et talle tundub, et paljud inimesed postitavad oma elu kohta sotsiaalmeediasse liiga palju infot, sh fotosid, sest nad soovivad saada teiste tunnustust, reaktsioone (nt meeldimisi) ega mõtle seejuures oma digitaalse jalajälje peale ega sellele, et sellist infot tuleks aeg-ajalt üle vaadata ning võib-olla ka kustutada, et tagada enda turvalisus.

Nooremad intervjueritavad mainisid aga paaril juhul seda, et aduvad TikToki kasutamisega kaasnevaid riske, kuid tajuvad samas ka sotsiaalset survet rakenduse kasutamiseks, kuna see on nende eakaaslaste seas niivõrd populaarne. Üks intervjueritavatest pole enda sõnul survele allunud, kuid teine tunnistas, et kasutab TikToki, olgugi et see teeb teda veidi murelikuks:

/.../ mis on tekitanud muret, on TikTok. Seda ei soovitata kasutada, kuna on mingeid kahtlusi infolekke kohta, aga samas see on selline platvorm, mis minuealiste seas on väga populaarne ja väga oluline. Ma ikkagi kasutan seda – see võib-olla on selline asi, mis tekitab natuke muret.

23-aastane intervjueritav

Puuduvad võimalused kasutada turvalisi lahendusi/seadmeid

Noorema vanusegrupi intervjuudel kerkis esile veel üks põhjus, miks alati küberturvaliselt ei käituta. Nimelt pole intervjueritavate sõnul alati võimalik kasutada digilahendusi, mis oleksid kontrollitud ja ohutud, sest puuduvad piisavad rahalised ressursid ja nii minnaksegi

teatud sisu tarbimiseks ebaturvalisemat teed. Üks valdkond, mille puhul turvalisuse vs rahalise kokkuhoiu dilemma tõusetub, on mõne intervjueeritava näitel meelelahutus (nt sarjade või filmide vaatamine).

Ma tuleks siin piraatluse juurde tagasi. Minu puhul on lihtsalt see, et meedia [tarbimine] maksab. Kahjuks ei ole alati seda, mille eest minna seda [sisu], kas siis Netflixist vaatama, kinno, mis iganes, onju. Minu puhul on lihtsalt see, et ma olen teadvustanud, kuidas nendel lehtedel [piraatlusega tegelevatel saitidel] navigeerida – pigem on see, et ma olen õppinud selles keskkonnas eksisteerima /.../ Aga minu jaoks on see... ma ei tea kui palju kalkuleeritud risk, aga teadlik risk.

24-aastane intervjueeritav

On märgiline, et lisaks meelelahutusliku sisu tarbimisele kerkis sama teema tugevalt esile ka hariduslikul eesmärgil kasutatava sisu puhul. Intervjueeritavad rõhutasid korduvalt seda, et õpingute käigus on neil tarvis olnud ligi pääseda teadusartiklitele või kasutada nt tekstitöötlusprogramme, mille originaalversioonidele pole olnud neil võimalik raha kulutada, mistõttu ongi mindud seda teed, et vajalik materjal laetakse alla saitidelt, mis ei pruugi olla sugugi turvalised.

Näiteks mul praegu ülikoolis on Microsoft olemas ja mul koolis ei olnud. Mul oli vaja Powerpointi ja neid asju – nagu Wordi... Ma laadisin seda alla mingilt kahtlaselt veebilehelt – lihtsalt, et kooliks on vaja. Kool ei anna mulle seda [vajalikku tarkvara].

21-aastane intervjueeritav

Oled sa siis ülikooliõpilane või midagi muud sarnast – raamatud on röögatult kallid, eriti veel akadeemiline kirjandus. Kui sa saad selle [vajaliku raamatu] kuskilt... ma ei tea, kunagi oli Z-library. /.../ Kui sul on võimalus alla laadida tasuta, siis sa kasutad seda. Aga see tuleb riskiga, et sa laed alla veel midagi peale selle kirjavara. See on ka vahepeal [koht], kus ma annan endale aru, et see [kahtlastelt saitidelt alla laadimine] ilmselt ei ole kõige turvalisem, aga samas – see on see *gamble* [õnnemäng], mida me lihtsalt võtame. Midagi pole parata.

24-aastane intervjueeritav

Lisaks nooremate intervjueeritavate poolt tõstatatud ligipääsu temale, mis puudutab tarkvara ja elektroonilist sisu, nentis üks vanema vanusegrupi esindaja intervjuul ka seda, et tema ei saa telefonis tarkvarauuendusi teha, kuna tegemist on liiga vana seadmega. Samas teab ta, et küberturvalisuse mõttes oleks uuenduste tegemine vajalik ning seega on ta oma ohutuse pärast ka natuke mures.

Muud ajendid küberhaavatavaks käitumiseks

Peale eeltoodu selgus intervjuudel veel mõningaid põhjuseid, miks intervjuueeritavate sõnul alati küberturvaliselt ei käituta. Järgnevalt nimetatud ajendid ei saanud laiapõhjalise arutelu osaliseks, pigem mainiti neid üksikutel kordadel, kuid peame siiski oluliseks need välja tuua:

- Küberturbe parimaid praktikaid ei rakendata nende kontode puhul, mis on kasutajale ebaolulised – nt ei kasutata tugevaid parooli või kaheastmelist autentimist vanade kontode puhul või juhul, kui tegemist on mõne veebilehega, kuhu pole sisestatud hulgaliselt isikuandmeid. Samas jääb seejuures alles risk, et mõnda sellist kontot häkkides saadakse ikkagi ligipääs ka inimeste teistele kontodele või andmetele, kuid seda ohtu ei tundu enamik teadvustavat.
- Usk, et tehnoloogia/tehnoloogilised lahendused on ise kaitse ohtude eest – mõnel juhul mainisid intervjuueeritavad, et nad eeldavad, et nende seadmed on juba (nt IT-salongi, mõne teenusepakkuja või varem iseenda poolt) seadistatud nii, et põhilised turvariskid on kaetud ja turvalisus seega justkui automaatselt tagatud.
- Puudub usaldus teatud tehnoloogiliste lahenduste või teenusepakkujate suhtes – mõned intervjuueeritavad tõdesid, et nad on (olnud) kahtlustavad nt kaheastmelise autentimise suhtes, kuna selle rakendamiseks tuleb veel rohkem enda infot välja anda (nt lisaks tavalisele salasõnale ka telefoninumber). Ka mainis osa intervjuueeritavaid, et paroolihaldur on miski, mida nad väga ei usalda, sest siis on kõik salasõnad ühes kohas koos ning nad ei usalda piisavalt vastava halduslahenduse pakkujat (kuidas on salasõnad ikkagi kaitstud, hallatud jne). Üks vanema eagrupi intervjuueeritav tõdes ka, et kui telekommunikatsiooniettevõtte pakuksid nt soodustusega meetmeid [nt tulemüür vms], mis mõjutaks inimesi küberturvaliselt käituma, siis oleks tema pigem kahtlev ega usuks telekommunikatsiooniettevõtete omakasupüüdmatut eesmärki. Niisiis viitab see, et turumajanduslikus süsteemis, kus inimestele püütakse alatasa midagi müüa, on tarbijatel kohati keeruline eristada olulist ebaolulisest ning eri toodete/teenuste müümise osas ollakse nii või naa keskmisest kahtlevam, rääkimata küberturbe valdkonnast, mis paljudele tundub tehniline ja keerukas.
- Psühholoogiline mõjutamine professionaalsete kelmidest poolt – vanema eagrupi intervjuudel nentisid intervjuueeritavad mõnel korral, et nt küberpettuste ohvriks võivad inimesed nii kergesti sattuda ka seetõttu, et kelmid on läinud üha osavamaks, manipuleerivad inimeste ja nende mõtlemisega väga professionaalselt ja isegi kui ohtudest ollakse teadlikud, võib juhtuda, et inimene jääb petturite juttu uskuma.

Vahekokkuvõte

Küberturvalisus on inimestele internetis toimetades küll oluline, kuid see, kui tihti teemat endale teadvustatakse ja kui sügavuti sellele mõeldakse, varieerub inimesti.

Aktiivselt teemale mõtlemist soodustab kokkupuude valdkonnaga (nt töö), isiklik ohutunne ning küberturvalisusalase info kajastamine (massi)meedias. Samas esineb osal inimestest n-õ passiivset usaldust ja harjumuslikku käitumist, mille tõttu jääb küberturvalisuse põhitõdede järgimine tahaplaanile, kuni tajutakse riski (nt kahtlasele veebilehele sattudes) või kui päriselt midagi enda või lähedastega juhtub.

Valdavalt hindavad inimesed oma teadlikkust küberturvalisusest piisavaks, kuid leidub ka neid, kelle arvates on kiiresti areneva digikeskkonna ja info ülekülluse tõttu keeruline end pidevalt viimaste arengute ja ohtudega kursis hoida. Isiklikku hinnangut oma piisavale või keskmisest kõrgemale teadlikkusele põhjendavad inimesed enamasti sellega, et nad teavad küberturvalise käitumise põhitõdesid ning toimetavad internetis ettevaatlikult ja tähelepanelikult. Niisiis leidub Eesti elanike küberkäitumises ka arengukohti, kuna inimestel puuduvad sageli süvendatud teadmised ning olemasolevaid teadmisi ei rakendata alati praktikas.

Inimesed tajuvad, et nende küberteadlikkus ja -käitumine on aja jooksul paranenud. Samas leidub ka neid, kelle küberkäitumine pole isiklikul hinnangul ajas märkimisväärselt muutunud, sest nad on enda sõnul kogu aeg olnud ettevaatlikud ja teadlikud internetikasutajad. Lisaks pole osa inimeste hinnangul nende küberteadlikkus küll vähenenud, kuid nende käitumine on siiski muutunud ajaga kohati hooletumaks, eelkõige mugavuse ja rutiinist tingitud automaatkäitumise tõttu.

Küberturvalisuse põhitõed, mida inimesed oma ohutuse tagamiseks järgivad, on mitmekesised: hoidumine kahtlastest veebilehtedest, sõnumitest ja e-kirjadest; turvaliste paroolide ja kaheastmelise autentimise kasutamine; tarkvarauuenduste tegemine ja turvalisust lisavate lahenduste kasutamine; ettevaatlikkus oma andmete jagamisel ja erinevate nõusolekute andmisel ning ka digitaalse materjali alla laadimisel ja selle kasutamisel. Eriti mõtlevad inimesed enda sõnul küberturvalisuse peale nende internetis tehtavate tegevuste puhul, kus ohtu võivad sattuda nende isiku- ja/või panga- ja krediitkaardiandmed. Samuti on internetist millegi allalaadimine tegevus, mille puhul turvalisust eriti silmas peetakse.

Samal ajal leidub Eesti elanike küberkäitumises endiselt ka puudujääke. Levinum probleem on nt turvaliste paroolide mittekasutamine. Ka ei kontrolli inimesed alati linke enne nendele klikkimist, ei logi külastatud veebilehtedel oma kontolt välja või lükkavad tarkvarauuenduste tegemist edasi jne. Küberturvalist käitumist ei piira seejuures enamasti mitte teadmatus, vaid olemasolevate teadmiste praktikas rakendamata jätmine.

Inimeste peamine ajend küberturvaliseks käitumiseks on hirm kaotada oma raha, andmed, identiteet või privaatsus. Samuti ajendavad inimesi küberturvaliselt käituma toetavad tehnilised/tehnoloogilised lahendused (nt paroolihaldur turvaliste paroolide genereerimiseks ja haldamiseks) ning kohustus küberturvalisi praktikaid järgida (nt

töökeskkonnas).

Ajendeid, miks inimesed käituvad küberhaavatavalt ega järgi küberturvalise käitumise põhitõdesid, on mitmekesiseid. Üks peamisi põhjuseid, miks küberturbe nõuandeid ei järgita, on inimeste arvates naiivsus või uskumus, et nemad ei satu internetis toimetades ohtu. Samuti pärsivad küberturvalist käitumist mugavus, laiskus, hooletus, väsimus ja ka kiirustamine ning asjaolu et küberturvalisusalased teadmised on kas puudulikud, ülehinnatud või praktikas rakendamata. Lisaks paneb sotsiaalne surve osa inimesi küberohtusid eirama ja käituma ebaturvalisemalt, kui muidu ehk inimesele omane oleks. Ka pole kõigil alati võimalik kasutada digilahendusi, mis oleksid kontrollitud ja ohutud, sest puuduvad piisavad rahalised ressursid ja nii minnaksegi teatud sisu tarbimiseks ebaturvalisemat teed.

3. Eesti elanike küberkäitumise mõjutamine: inimeste endi vaade

Olles käsitlenud seda, milline on Eesti elanike küberkäitumine, keskendume järgnevalt sellele, kuidas oleks võimalik inimeste käitumist mõjutada. Niisiis toome selles peatükis esmalt välja, kust inimesed saavad küberturvalisusalast infot, kas seda on piisavalt ja/või mis teemadel tuleks rohkem teavet jagada. Seejärel anname ülevaate sellest, mis võiks motiveerida inimesi küberturvalisusele senisest enam tähelepanu pöörama ning milliseid kanaleid, formaate ja sõnumeid võiks üldse asjakohase info levitamiseks kasutada.

Siinkohal on oluline meeles pidada, et selle peatüki sisend on intervjuude käigus kogutud materjal ehk just Eesti elanike endi vaade sellele, missugust infot ja mil moel nad küberturvalisuse teemal saada sooviksid ning millised võiksid olla nende motivaatorid küberturvalisema käitumise saavutamisel.

3.1. Kust saavad inimesed küberturvalisusalast infot?

Intervjueeritavatega vesteldes selgus, et Eesti inimesed saavad küberturvalisuse kohta informatsiooni erinevatest allikatest, alates massimeediast kuni pere, sõprade või töökohani. Järgnevalt toome välja kõik intervjuudel mainitud infoallikad, olles need koondatud suuremate alamteemade alla.

Massimeedia, sh digitaalne massimeedia kui infoallikas

Kõikide uuringusse kaasatud vanuserühmade esindajate puhul leidis mitmeid intervjueeritavaid, kes ütlesid, et nendeni jõuab küberturvalisusalane info massimeedia, sh veebiväljaannete ja -saitide vahendusel. Intervjueeritavad mainisid, et saavad teavet nii uudiseid (nt keskmise vanuserühma esindajad mainisid korduvalt, et uudislugudest saab infot levinumate petuskeemide kohta) kui ka just küberturvalisusalaseid artikleid lugedes. Vanema ja keskmise eagrupi esindajad mainisid seejuures konkreetsete portaalidena, mida nad kasutavad, Delfit ja ERR-i (sh Novaatorit).

Lisaks mainisid nii noorema kui vanema eagrupi esindajad paari korral televisiooni kui üht endale olulist infoallikat. Paar 23-aastast intervjueeritavat tõstsid nt esile, et neile on küberturbe teemal infot meelde jäänud telekanalite hommikuprogramme jälgides või nt „Ringvaatest“.

Üks nooremaste eagrupi kuuluv intervjueeritav tõdes infoallikatest rääkides, et tema hinnangul on mõjus, kui teavet jagatakse eri kanalites ja formaatides nii, et on tagatud vaheldusrikkus:

./.../ mulle mõjub vist tervikuna see [informeerimine]. Mõnikord ongi mingi välireklaam ja mõnikord on mingi telefonireklaam ja mõnikord on teelugu.

23-aastane intervjuueritav

Rääkides konkreetsetelt teavitusemeediast, siis mõned vanemad intervjuueritavad tõstsid esile, et nad on näinud mini-saatesarja „IT-vaatlik“. Seejuures neist üks lihtsalt mainis, et on sarja näinud; üks nimetas seda „armsaks saateks“, kuid üks oli ka kriitiline ja leidis, et sari on elukauge ega paelu teda kui vaatajat.

Nooremate intervjuueritavate seas oli mitmeid, kes tõdesid, et nemad on märganud teemakohaseid avalikke kampaaniaid. Ka üks keskmise eagrupi esindaja meenutas, et ta on silmanud kampaaniat „Ole IT-vaatlik!“, kuid tema hinnangul kampaania sõnumid talle sisulist teavet eriti ei andnud.

Ühtlasi meenus ühel intervjuueritaval keskmisest eagrupist, et ta on märganud ka ennetusportaal itvaatlik.ee veebireklaami ja sellest ajendatuna portaali külasthanud, kuid oluliselt sisulisemalt süvenemist teemasse see tema hinnangul kaasa ei toonud. Paar intervjuueritavat tõid aga välja, et nad on teinud itvaatlik.ee portaalis testi oma teadmiste kontrollimiseks. Veel kaks keskmise eagrupi kuuluvat intervjuueritavat lisasid, et nemad lapsevanemana on küberturvalisuse teemal infot saanud ka projekti „Targalt internetis“ veebilehe kaudu.

Sotsiaalmeedia kui infoallikas

Lisaks massimeediale mainisid intervjuueritavad korduvalt, et küberturvalisusalane info jõuab nendeni ka sotsiaalmeedia vahendusel. Eriti tõstsid seda infoallikana esile nooremad intervjuueritavad. Konkreetsetest platvormidest mainisid nad nt korduvalt Youtube'i ning korra ka TikToki. Esimese puhul tõdesid noored, et seal vaatavad nad ka pikemaid teemakohaseid videosid, et end üldiselt valdkonnaga kursis hoida ja/või mingeid teemasid paremini mõista:

Ja [saan infot ka] YouTube'ist – eriti mingid pikemad videod, mida ma vaatan niisama põnevuse pärast. ./.../ Sellest [videote vaatamise tagajärjena] hakkad ka kuidagi teise pilguga vaatama võib-olla neid asju.

21-aastane intervjuueritav

Kõikide uuringusse kaasatud vanuserühmade esindajate hulgas oli intervjuueritavaid, kes nimetasid ühe viisina, kuidas nad sotsiaalmeedia vahendusel küberturvalisuse kohta infot saavad, et vastavateemalised postitused jooksevad aeg-ajalt nt nende sotsiaalmeedia kontode uudisvoost läbi. Samuti mainisid nii mõnedki intervjuueritavad (eri vanuserühmadest), et nad jälgivad ise sel teemal teatud spetsiaalseid grupe või kontosid. Nt keskmisest eagrupist tõstis osa intervjuueritavad muuhulgas esile, et nemad jälgivad sotsiaalmeedias veebikonstaablite kontosid, et end infoga kursis hoida.

Üks 24-aastane intervjueritav tõstis eraldi esile ka riigiametite ja ministeeriumite sotsiaalmeedia postitusi, mis tema hinnangul on ajas paremaks läinud. Küll aga ei selgunud, kas ta peab seejuures silmas, et postitused on pilkupüüdvamad, sisulised või praktiliselt kasulikumad.

Teised inimesed kui infoallikas

Küberturvalisusalase info levimisel on oluline roll ka teistel inimestel, nt lähedastel, sõpradel või kolleegidel. Mitmed noored mainisid intervjuudel, et neid on küberturvalisemalt käituma suunanud lapsevanemad, kes on kas ise oma kompetentside ja käitumisega eeskujuks või kes ongi jaganud konkreetseid nõuandeid ja õpetussõnu. Üks noor meenutas, et talle ostis ema kunagi ka vastavateemalise raamatu, mida ta siis luges. Seda, et küberturvalisuse teemal saadakse infot (või vahetatakse seda omavahel) tavaliselt või sõpradelt, tõid noored välja vähem.

Ühtlasi leidis paar noorema eagrupi intervjueritavat, kes nimetasid ühe infoallikana projekti „Targalt internetis“: üks tõdes, et ta teab projekti lähedalt, kuna tema tutvusringkonda kuulusid sellega tegelevad inimesed; teine aga meenutas, et tal oli kunagi projekti tegelusvihik, mida sai täita ja seeläbi temasse süveneda.

Küberturvalisuse teemaga kursis olemisel tõstsid intervjuudel just lähedaste inimeste rolli esile ka keskmise ja vanema eagrupi esindajad. Üksikutel juhtudel mainisid intervjueritavad, et teemast räägitakse sõpraderingis või et nõu saab küsida nt kolleegidelt, rohkem tõid nad aga välja pereliikmete tähtsust info ja nõuannete saamisel. Paar naissoost intervjueritavat tõdesid, et nemad küsivad küberturvalisuse teemal vajadusel nõu abikaasalt, mis on üheltpoolt küll positiivne, kuid võib teisalt tekitada olukorra, kus loodetaksegi teise inimese pädevusele. Ühtlasi võib see viidata soolistatud muustrile, kus mehi sotsialiseeritakse end küberasjades harima ja naisi pigem selles suunas, et nad ei peagi teemast aru saama.

Minu peamine teejuht on mu abikaasa, sest ta on lihtsalt nii palju rohkem huvitatud ja kursis nende [küberturbe] asjadega. Ja võib-olla olen ka viinud ennast teatud õpitud abituse olukorda. Ma olengi kuidagi harjunud sellega, et tema ütleb ja siis ma nii teen või ei tee. Või ma pean temaga nõu.

31-aastane intervjueritav

Vanemas eagrupis jäi intervjuudest kõlama, et vanemad inimesed loodavad kahtluse või oskamatus korral sageli nooremate sugulaste (eeskätt oma laste) abile ning saavad nende käest vajalikku küberturvalisusalast nõu. Samas peegeldab ühe intervjueritava öeldu ka seda, et nooremad sugulased ei pruugi alati tahta, jaksata või osata vanemale inimesele piisavalt selgitusi jagada ega tee ilmselt ka kindlaks, et edastatud info on tõesti arusaadav ja teine inimene nõu ka (edaspidi) rakendab:

Lastelt küsin ikka nõu, aga nad võtavad kordades lihtsamalt kõike. Ütlevad “No ja mamma, mida sa jälle pabistad?”
59-aastane intervjueritav

(Kõrg)kool kui infoallikas

Suurem osa uuringu käigus intervjueritud noorema vanusegrupi esindajatest tõdes, et nad on küberturvalisuse kohta infot saanud ka kooli⁹ kaudu, kas siis informaatika õppeaine raames või spetsiaalsetel küberturvalisuse loengutel. Neid noori, kes ütlesid, et koolis küberturvalisusest eriti ei räägita/räägitud, oli intervjueritavate seas vaid mõni. Üks neist tunnistas seejuures, et teemat küll käsitleti koolis, ent tema meelest liiga hilja:

Ma ei mäleta, kuidas algklassides oli. Gümnaasiumis muidugi oli ka, räägiti [küberturvalisusest]. Selleks ajaks kui informaatika tund tuli, oli kõik juba nii normaalseks saanud, et see tundus tagurlik või et “kus te 10 aastat tagasi olite, et nüüd me hakkame sellest rääkima!”
'23-aastane intervjueritav

Ka üks 16-aastane intervjueritav tõdes, et põhikoolis käsitlesid nad informaatika tundides teemasid (nt turvalised paroolid), mille kohta ta oli juba niikuinii kuulnud ning oleks seega eelistanud õppida midagi uut.

Üks 21-aastane intervjueritav viitas, et ta on saanud infot ka ülikoolist, sest võtab vabatahtlikult juurde mõningaid IT-alaseid õppeaineid.

Töökoht kui infoallikas

Kõikide vanusegruppide puhul mainisid intervjuudel osalejad ka seda, et on küberturvalisusalast infot saanud töökohta kaudu. Noorema vanusegrupi esindajad mainisid seda mõnel korral, sh et infot on saadud ka praktiliselt olles. Keskmise ja vanema eärühma esindajad nimetasid töökohta kui üht infoallikat korduvalt, tuues näidetena välja, et on tööl osalenud küberturbe koolitustel, läbinud IT-teste ning et töökohad on levitanud küberturvalisusalaste kampaaniate infot. Need, kes mainisid, et nad saavad infot ka töö kaudu, tõdesid, et koolitused või muul viisil info jagamine on pidev, mitte et oleks kunagi toimunud nt üks koolitus või muu teemakohane ettevõtmine.

Üks vanema eärühma esindajatest tõstis intervjuul esile, et on saanud koolitusel osaleda ka Töötukassa kaudu, kuna ta on töötuna arvel. Vanema vanuserühma esindajatest mainis koolitustel osalemist veel paar inimest, kuid kõigi puhul ei selgunud, kas tegemist on avalike koolitustega, kuhu on end ise kirja pandud, või pidasid intervjueritavad silmas siiski töökohta kaudu korraldatud koolitusi.

⁹ Üldjuhul pidasid intervjueritavad siinkohal silmas üldhariduskooli, üksikutel juhtudel kõrgkooli.

3.2. Kas küberturvalisusalast infot on inimeste hinnangul piisavalt ja mis teemadel tuleks seda lisaks jagada?

Uurisime intervjuude käigus inimestelt ka seda, kas küberturvalisusalast infot on nende hinnangul piisavalt või mitte ning kas on konkreetseid küberturvalisusalaseid teemasid, mille kohta nad rohkem teavet sooviksid.

3.2.1. Info piisavus

Suurem osa uuringu käigus intervjuueeritud Eesti elanikest leidis, et küberturvalisusalast infot on piisavalt. Samas tõdesid mitmed neist seda, et **olgugi et infot on piisavalt, ei pruugi see inimestele alati ette sattuda ja huvi või mure korral tuleb sel juhul vajalikku teavet ise otsida**. Info kättesaadavust omal initsiatiivil otsimise korral pidasid intervjuueeritavad pigem heaks, küll aga nimetasidki murekohana just seda, et tõenäoliselt need, kel küberturvalisusalast teavet enim vaja oleks, sageli teemast ei huvitu ning seega asjakohase infoga kokku ei puutu.

/.../ kui sa just ise selle [küberturvalisusalase info] vastu huvi ei tunne, siis seda väga kusažil ette ei tule.
18-aastane intervjuueeritav

/.../ seda [küberturvalisusalast] infot on piisavalt, kui keegi tunneb huvi või tahab ennast sellega kurssi viia või tekivad mingid küsimused, siis selle info leiab küll. Kuidas see info jõuaks nende kasutajateni, kellel seda kõige rohkem vaja on ja kes võib-olla ise ei oska automaatselt seda tahta või osata otsida – see on teine teema.
37-aastane intervjuueeritav

/.../ seda [küberturvalisusalast] infot on tegelikult piisavalt, aga inimestel ei ole lihtsalt huvi või arusaama, et see on oluline info ja seda [infot] ei tõsteta piisavalt esile. Tegelikult see IT-vaatlik ja kõik need teemad, mis meedias on, ja intervjuud, mis antakse teles ja nii edasi... Tegelikult seda infot tuleb peale väga palju /.../ Aga lihtsalt inimesed ei kuula, ma arvan. Probleem on pigem sealpool.
39-aastane intervjuueeritav

Ka uuringu käigus tehtud intervjuudel ilmnes, kuidas küberturvalisusalane info on küll olemas, kuid ei jõua alati inimesteni, isegi kui tegu on pigem teadlike ja teemast huvitatutega. Nimelt mainis üks intervjuul osaleja ühes noorema vanusegrupi fookusrühmaintervjuus mobiilirakenduse „Ole valmis!“ küberhügieeni alusõppe moodulit, misjärel üks teine osaleja tunnistas, et tal polnud aimugi selle materjali olemasolust nimetatud rakenduses:

Aitäh sulle, [nimetab teist intervjuul osalejat], "Ole valmis!" äpi küberturvalisuse sektsiooni [mainimise] eest. Vaatasin, kontrollisin üle, täiesti on olemas. Nüüd olen ka targem. Aga tõesti, mida ma näen ka enda näitel väga hästi, on see, et [küberturvalisusalased] materjalid on kõik olemas, aga mingil põhjusel need ei jõua minuni.

24-aastane intervjueritav

Mõned noorema vanusegrupi intervjueritavad tõid ühtlasi välja, et nende hinnangul saavad avalikkuses ülekaalukalt palju kajastust erinevad petuskeemid, kuid üldist küberturvalisusalast ennetusele suunatud infot leidub pigem vähem. See võib viidata ka sellele, et noorte hinnangul räägitakse pettustest nii palju, et muud küberturvalisusega seondud jääb varju:

Sotsiaalmeedias või niimoodi ma ikkagi ei satu väga selle teema [küberturvalisuse] peale. Kui see just ei olegi jälle mingi petuskeemide teema. Uudistest pole silma hakanud. Nii väga sellest [küberturvalisusest] ei räägita ka tutvusringkonnas. Ehk siis ongi juhuslikud kohad, töö, kool, kust ma kuulen neist teemadest üldse.

23-aastane intervjueritav

Üks 24-aastane intervjueritav pidas küberturvalisusalast infot ka killustatuks.

Intervjuude põhjal võib öelda, et **veidi vastakaid tundeid tekitab Eesti elanikes see, kui palju tuleks küberturvalisusalast infot avalikkuses ikka ja jälle üle korrata**. Nt intervjueritud PPA esindaja tõdes oma kogemusele tuginedes, et küberturvalisusest tuleb rääkida järjepidevalt, sest ikka leidub neid inimesi, kes pole vajalikust infost üldse kuulnud. Ka üks vanema eagrupi intervjueritav leidis, et kahju pidev teavitamine kindlasti ei tee, ning üks 22-aastane intervjuul osaleja tõdes, et tema ei taju, et küberturvalisusalaseid põhitõdesid aina korratakse ja korratakse, vaid pigem juhtub ta vastavasisuliselt reklaame nägema heal juhul kord kuus.

Samal ajal leidsid siiski ka mõned intervjueritavad (samuti eri vanuserühmadest), kes leidsid, et küberturvalisusalast infot on liiga palju ja see hakkab seetõttu muutuma tüütavaks või inimesed lihtsalt ei märka seda enam ja nii-öelda lülitavad end infovoost välja:

Ma arvan, et on küll [piisavalt küberturvalisusalast infot saadaval]. /.../ Kohati tundub, et isegi on nii palju, et kui midagi on palju, siis see muutub taustaks lihtsalt. /.../ Pigem ongi alati küsimus, kuidas selle infoga inimesteni jõuda.

62-aastane intervjueritav

Lisaks kerkis intervjuudel seoses info piisavusega esile ka mõningaid muid nüansse. Üks aspekt, mida mõned intervjueritavad esile tõid, oli **eestikeelse info kättesaadavus**. Nt paar noorema eagrupi esindajat tõdesid, et eestikeelset küberturvalisusalast teavet leidub nende hinnangul märksa vähem kui ingliskeelset. Üks 59-aastane intervjueritav tunnistas, et ise tema teemakohast infot otsima ei vaevu, aga ühtlasi usub ta, et see oleks niikuinii inglise

keeles. Keskmise vanusegrupi intervjuudel mainis keele aspekti samuti paar intervjueeritavat: üks neist leidis, et vaatamata muidu heale inglise keele oskusele eelistaks tema küberturvalisusalast infot saada eesti keeles; teise hinnangul ei ole vahet, mis keeles infot leidub ja et tema vanemad ei oska küll inglise keelt, kuid usutavasti ei pühendaks nad teema uurimisele aega niikuinii, olenemata kättesaadavate materjalide keelest.

Paar intervjueeritavat avaldasid ka arvamust, et **jagatav teave (sh koolitustel) võiks olla alati väärske ja ajakajaline**, puudutades sh sotsiaalmeediaga seonduvaid ohte, tehisaru jms.

Ma olen läbinud ka mingi koolituse küberturvalisuse kohta. /.../ võib-olla on ka probleem selles, et need tänased koolitused on natukene aegunud, et nad ei puuduta ohte, mis võivad ümbritseda meid sotsiaalmeedias ja võib-olla siis tehisaruga [seoses]. Need koolitused, millest mina olen teadlik, pigem on sellised oldschool [vanamoodsad] ja räägivadki rohkem linkidest, meilipettustest.

23-aastane intervjueeritav

3.2.2. Teemad, millest tahaks rohkem teada

Samuti küsisime intervjuude käigus inimestelt seda, millist tuge nad küberturvalise käitumise rakendamisel vajavad, sh millistel teemadel tuleks nende meelest senisest rohkem informatsiooni jagada.

Tehisaru

Kõikide eagruppide intervjueeritavate poolt tõsteti ühe teemana, mis külvab segadust ja tekitab küsimusi, esile tehisaruga¹⁰ seonduv. Intervjueeritavad tunnistasid, et nad ei saa päris hästi aru, kuidas tehisaru ikkagi toimib, mistõttu tekitab sellega seonduv ka ebalust. Korduvalt mainisid eri vanuses inimesed, et nad kasutavad tehisaru, kuid ei saa lõpuni aru, kuidas ja milline digitaalne jalajälg nende päringutest jääb, kuidas tehisaru andmeid talletab ja mida tuleks oma turvalisuse tagamiseks täpsemalt silmas pidada.

(Isiku)andmete kaitsmine ja privaatsus

Osa noorema ja keskmise eagrupi intervjueeritavaid tunnistas, et nemad vajaksid rohkem teavet ja paremat arusaamist selle kohta, kuidas erinevaid rakendusi ja veebipõhiseid teenuseid kasutades inimeste andmeid kogutakse, säilitatakse ja kasutatakse. Mitmed tõdesid, et praegu nad teemat lõpuni ei mõista, kuid kasutavad rakendusi/teenuseid sellest hoolimata:

¹⁰ Tehisaru all peame siinkohal silmas peamiselt suurtel keelemudelitel põhinevaid juturoboteid nagu ChatGPT, mille kasutamist intervjueeritavad kirjeldasid.

Paljude inimeste ja ka minu jaoks on segadust tekitav kõik need nõusolekud, mis me anname sotsiaalmeedias /.../ tehes kontot või üldse. Vahepeal on need privaatsussätted ja kõik see, kus pannakse siis pikk leping sulle ette, kus sa pead lõpus siis selle [nõusoleku] tärnikesse panema. /.../ olen päris tihti pannud selle tärnikesse ka niimoodi, et ma seda [infot] läbi ei loe ja siis hiljem tegelikult võib tulla päris suur üllatus, et minu andmeid võib niimoodi kasutada.

23-aastane intervjuueritav

Lisaks töid mitmed (just keskmise vanusegrupi) intervjuueritavad välja, et nende jaoks on segane see, kas ja kui palju saavad eri seadmed, rakendused ja/või veebilehed kasutajate tegevust jälgida. Pealtkuulamine, kaamera kaudu inimeste jälgimine jms on miski, mis tekitab nii mõneski inimeses segadust ja nad ei saa aru, kas nende hirmudel on alust või mitte:

See on minu arust nii vandenõudega läbi põimunud teema, et ma ei saa aru, kust jookseb see reaalsus, mis mind puudutab – näiteks igasugu kaamerad ja mikrofonid ja mingi pealtkuulamine ja vaatamine. Vahepeal oli hästi teemas see, et plaastriga pandi oma neid [arvutite] esikaameraid kinni. Mul on ka näiteks see [kaamera] klappikene siin. Aga ma panin selle lihtsalt sellepärast [kinni], et ma sain ja ma mõtlesin, et sama hästi võin selle siis [kinni] panna.

31-aastane intervjuueritav

Ise võib-olla olen vähem tähele pannud, aga teised räägivad, et “Ah, rääkisin mingisugustest katuseterrassidest sõbraga ja näed, kohe telefon pakkus selliseid asju [reklaamides]!”. Kui palju see siis on see, et sind kuulatakse [seadme poolt pealt] ja siis pakutakse [neid asju]?

38-aastane intervjuueritav

Muuhulgas leidis üks intervjuueritav, et vaadates inimeste üldist internetikäitumist, võiks rohkem jagada infot ka selle kohta, kuidas hoiustada oma pilte ja videosid nii, et need ei lekiks (kellele üldse materjali saata; millises keskkonnas ja kuidas ning kui kaua säilitada jms).

Olgugi et vanema eagrupi esindajad ei maininud uuringu käigus andmete kaitsmise ja oma privaatsuse tagamisega seonduvat kui teemat, mille kohta nad rohkem infot sooviksid, ei saa eeldada, et nende teadmised on selles vallas oluliselt paremad kui teiste eagruppide esindajate puhul. Vastupidi, võib ka olla, et vanemad intervjuueritavad ei tõstatanud teemat, kuna see on miski, mille peale nad internetis toimetades üldse nii palju ei mõtle, sest teadlikkus on selles osas madalam ja nad ei oskagi teemaga seoses riski näha.

Turvalised paroolid

Ka turvaliste paroolide loomine ning haldamine on miski, millest võiks mõne intervjuueritava sõnul rääkida rohkem. Nt paar intervjuueritavat selgitasid, et nad tahaksid küll erinevaid turvalisi salasõnu kasutada, kuid see, kuidas neid täpselt genereerida ja hiljem meeles pidada,

tekitab neis küsimusi. Järgnevad tsitaadid peegeldavad ühtlasi seda, et paroolihaldurite kasutamine ei ole alati inimestele kõige harjumuspärasem.

Google ja Apple näiteks /.../ kui teed endale konto, siis ta alati pakub sulle kõige pikema, kõige suvalisema parooli, mida sa mitte kunagi ei mäleta. Võib-olla oleks kasulik, kui nad õpetaks sulle, et võib-olla tee parool endale selgeks niimoodi, et paned selle riimuma millegagi – teed mingi luuletuse, et sa mäletad enda parooli. /.../ Mul ongi nii palju neid sama parooliga kontosid lihtsalt sellepärast, et mulle ei ole häid ideid antud, kuidas need [paroolid] kõik meele jätta. /.../ Oleks kasulik, kui oleks mingi teine nõuanne, kui lihtsalt et pane mingid numbrid [parooli] sisse ja mingid hüüumärgid ja küsimärgid parooli lõppu. See ei ole väga kasulik tavainimesele, sest tavainimene ei viitsigi panna endale kõige turvalisemat parooli.

16-aastane intervjueritav

Puudu on sellest infost, kuidas siis ikkagi neid erinevaid paroole panna niimoodi [turvaliselt]. Tähendab [turvalisi] paroole võib panna, sa võid ju erinevaid kombinatsioone välja mõelda ja tegelikult internet pakub ise ka seda [paroolide genereerimist]. Lihtsalt küsimus on, kuidas ma seda meeles pean pidama või kus kohas neid [paroole] siis hoida, kust ma neid vaatan siis, kui mul neid vaja on. Ma arvan, et kui see oleks inimestel selgem, et siis seda [turvalisi paroole] kasutatakse rohkem.

56-aastane intervjueritav

Muud tehnoloogia ja seadmetega seotud teemad

Lisaks eeltoodule selgus intervjuudel veel mõningaid küberturvalisusega seotud teemasid, mille kohta võiks intervjueritavate meelest rohkem informatsiooni jagada. Järgnevalt nimetatud teemasid mainiti intervjuudel pigem üksikutel kordadel, kuid peame siiski tähtsaks need välja tuua:

- VPN-i kasutamine – võiks olla selgem, kas VPN-i peaks kasutama igäüks ehk kas see on ka tavakasutaja jaoks turvalisuse tagamisel standard või pigem miski, mida kasutada vastavalt vajadusele.
- WiFi turvalisus – rohkem teavet selle kohta, kas (avalikku) WiFi-t on turvaline kasutada, kas osa ruutereid on ohutumad kasutada kui teised ja mille järgi neid valida.
- Viirusetõrje tarkvara – kasutaja saab küll nt aru, kas viirusetõrje programm on töökorras (jälgib, kas programmi logo kuvab nii, nagu peaks), kuid ei tea täpsemalt selle toimimisest, ei oska vajadusel reageerida ja kontrollida, kas kõik on korras.
- Telefoni turvalisus – kas telefoni kui digiseadet kasutades peab ka kartma viirusi; kui turvaline on olla telefoniga avalikus võrgus jms.

Küberturvalisuse võtmesammude rõhutamine vs rohkem tehnilist ja detailset infot

Intervjuudest selgus ka see, et eri sihtrühmade infovajadus, sh info detailsusastme osas võib olla erinev. Nt keskmisest eagrupidist tõid paar intervjuueeritavat välja, et kuna tehnoloogia on viimaste aastakümnetega tormiliselt arenenud ja väga palju on muutunud, tunnevad nad, et on hulgaliselt asju, mida tuleks oma turvalisuse tagamiseks teha, kuid lõpuks jääb segaseks, mis on need võtmesammud, mis tuleb astuda, et baastase oleks saavutatud. Seega oleks vaja rohkem teavet küberturvalisuse põhitõdedest.

Mulle tundub, et vanasti see [küberturvalisuse] teema oli palju selgem ja lineaarsem. Peamiselt sellepärast, et tehnoloogia oli nii palju lihtsam. Ma mäletan, et keskkooli lõpus ma olin väga võidukas, et viirusetõrje [on olemas], ei vajuta [kahtlastele] linkidele meilides – ja korras! Ja võib-olla, kui sa oled uhke, siis paned mingi *firewalli* [tulemüüri] veel. Nüüd mulle tundub, et see ülevaade sellest, mis on õige või mis töötab või mis on see hea baasmõte – see on hästi palju hägustunud. Tehniliselt ma võiksin teha ju nii palju asju, et... /.../ Mis on õige ja hea mõte või mis on lihtsad võtmesammud, mis teha, see ei ole selge.

37-aastane intervjuueeritav

Seevastu noorema vanuserühma seas oli mitu intervjuueeritavat, kes rõhutasid, et üldised küberturvalisusalased soovitused ja põhiinfo on olemas (ja neid kohati isegi ära tüüdanud), kuid mida nad rohkem näha sooviksid, on süvitsiminev, nii-öelda edasijõudnute taseme informatsioon.

Seal [itvaatlik.ee ennetusportaalil] ongi sellised hästi üldised nõuanded, mis on head nõuanded, aga võiks ka olla selliseid rohkem tehnilisemaid ja detailsemaid, sest palju asju... /.../ neid ma juba tean ja neid meetmeid ka rakendan. [Need] sobiks hästi algajatele, aga mitte juba rohkem kogenumatele. /.../ Muuta siis põnevamaks seda infot.

18-aastane intervjuueeritav

Kui sulle lihtsalt öeldakse, et kasuta [paroolis] hüüumärki, sa ei saa tegelikult aru, miks ilma selle hüüumärgita see tõenäosus, et ta [häkker] arvab selle parooli ära [on suurem] /.../ Taustateadmine mõnikord seletab, miks sa peaksid midagi tegema ja siis see tegemine muutub ka palju lihtsamaks, sest see ei tundu mingi mõttetute tegevus.

21-aastane intervjuueeritav

Osa intervjuueeritud noori tunnistas ka, et kui jagatakse vaid küberturvalisusalast baasinfot, võib tekkida tunne, et kõike olulist oma turvalisuse tagamiseks tehakse juba niigi ning seega kaob huvi teema vastu. See omakorda võib aga viia ka valvsuse kadumiseni.

/.../ isegi olen külastanud [itvaatlik.ee ennetusportaali]. Aga need soovitusel [portaalis] olid pigem üldisemad ja mul oli tunne, et "aa, ma tean seda".

21-aastane intervjueritav

/.../ see info, mis antakse edasi, ongi väga üldine, väga lihtne, mis on mõnes mõttes väga hea asi, aga kui sa juba rakendad mingeid meetmeid, siis tihti sa võid mingi lehekülje soovitusel läbi lugeda ja siis mõelda, et ma ei saanudki midagi uut teada. Ja siis kaob huvi selliste lehekülgede vastu ära. /.../ See [küberturvalisusalane] info võiks olla mitmekesisem ja seda võiks olla lihtsamat, keerulisemat. Tihti inimesi lihtsalt ei huvita, kui nad on juba piisavalt palju kordi midagi kuulnud.

19-aastane intervjueritav

Mida teha, kui internetis toimetades midagi juhtub?

Lisaks kerkis keskmise eagrupi intervjuudel ühe olulise nüansina esile see, et infot küberohtude vältimise kohta võib küll olla pigem piisavalt, ent vähem on teavet selle kohta, mida teha siis, kui midagi on juba juhtunud. Mõne intervjueritava näitel võib öelda, et inimesed ei tea, kas ja mis hetkeni saavad pangad nt kahtlased rahaülekanded tühistada; kuhu pöörduda siis, kui kaotsi pole läinud mitte raha, vaid identiteet jms.

/.../ praegu [jagatava informatsiooniga] on nii, et „olge ettevaatlikud“. Ja siis kui [midagi] juhtub, siis ongi kõik. /.../ Tegelikult ma tean, et pankadel on võimalus teha raha tagasikutsumised mingitel hetkedel, aga sellest väga palju ei räägita, sest et see ilmselt on keeruline ja kallid. Aga mis on need asjad [mida tuleb teha] – kas ma peaksin näiteks politseisse või veebikonstaablile kirjutama, et mul juhtus selline asi, kas ma peaks politseisse avalduse tegema kui ma näen... Kui raha on kadunud, siis see on selge, aga kui mu identiteet varastatakse, mis on ka tõsine... Mis need sammud võiks olla [mida teha], kui peaks juhtuma?

39-aastane intervjueritav

Samuti mainis üks intervjueritavatest, et senisest enam tuleks mõelda sellele, kuidas küberkuritegude ohvreid toetada.

3.3. Mis motiveeriks inimesi küberturvalisusele rohkem tähelepanu pöörama?

Selleks, et saada teada, kuidas võiks inimesi mõjutada käituma küberturvalisemalt, uurisime neilt intervjuude raames ühtlasi, mis innustaks neid nende endi hinnangul küberturvalisusele rohkem tähelepanu pöörama. Eristame seejuures inimeste sisemist motivatsiooni tõstvaid tegureid ja väliseid motivaatoreid.

3.3.1. Inimeste sisemist motivatsiooni tõstvad tegurid

Isiklik kokkupuude ohuga ja/või elulised näited ja kogemuslood

Uuringu käigus tehtud intervjuudest nähtub, et kõige mõjukamaks ja enim mainitud motivaatoriks, mis paneks intervjuueeritavaid (või nende hinnangul inimesi üldiselt) küberturvalisusele rohkem tähelepanu pöörama, on reaalne eluline näide ehk isiklik kogemus või kellegi teise (sh lähedase) kogemusloost osa saamine.

Kõigi uuringusse kaasatud vanuserühmade esindajad kinnitasid üksmeelselt, et küberturvalisele motiveeriks enam tähelepanu pöörama **isiklik hoiatav kogemus küberintsidendiga**. Sageli tajuvad inimesed (sh intervjuueeritavad ise) küberturvalisust kui teemat liiga kauge ja teoreetilisena, kuni midagi just endaga juhtub.

See vist ikka kipub olema niimoodi, et õpitakse enda vigadest, mitte teiste omadest, et kui midagi juhtub, siis hakkad mõtlema, mida saaks ise paremini teha tõesti.

42-aastane intervjuueeritav

/.../ kui sa saad pihta ja kõik [langed küberintsidendi ohvriks], siis elu õpetab. Jah, kui sul realselt midagi juhtub, /.../ siis sa saad aru. Et see võidetud aeg [nt kaheastmelist autentimist mitte kasutades] ei õigustanud ennast.

62-aastane intervjuueeritav

Intervjuueeritud küberturvalisuse ekspert tõdes samuti, et isiklik praktiline kogemus võiks innustada inimesi küberturvalisusele enam tähelepanu pöörama. Kui inimene realselt tajuks, mis tunne on ohvriks sattuda, siis ta õpiks sellest – isegi kui kogemus on stimuleeritud. Seejuures pakkus küberturvalisuse ekspert välja, et stimuleeritud kogemuse võiks inimestele anda nt teemakohase mängu või mingi stsenaariumi abil (nt virtuaalreaalsusega).

Meil ei ole praktilisi kogemusi. Need, kes on saanud praktilised kogemused, need juba teavad. Ehk siis kõigepealt tuleks viia inimesed sinna olukorda, kus nad saavad praktilise kogemuse – on see mingi mäng; on see mingisugune stsenaarium, mida me kõik läbi mängime, kus ma saan olla ohvri rollis.

küberturvalisuse ekspert

Mitu noorema vanusegrupi intervjuueeritavat nõustus, et toimida võiks n-ö šokiteraapia, et tehakse mingi test või osaletakse (üli)kooli poolt korraldatud küberõppuses ja saadakse selle kaudu teada, kas teadlikkus on piisav või mindi nt petukirja õnge vms. See võimaldaks teoreetilisi teadmisi rakendada ja läbi ohutute eksimuste õppida. Täpsemalt vaata selle idee kohta peatükist 3.4.1.

Ka **lähedaste ja tuttavate kogemuslood** motiveeriks intervjueeritavate sõnul neid küberturvalisusele rohkem tähelepanu pöörama, sest need lood aitaksid riske teadvustada ja mõista, et tegu pole millegagi, mis juhtub kuskil kaugel kellegi teisega, vaid see on igapäevaste reaalsete mõjutava võiv oht. Usaldusväärse ja samastatava ohvriga juhtum aitab murda eksiartvamust, et “mina olen ettevaatlik ja teadlik, minuga seda ei juhtu” (seda uskumust avasime ka juba eelpool peatükis 2.5).

/.../ kui keegi lähiringkonnas ikkagi satuks [nt petuskeemi ohvriks], siis jääks küll rohkem mõtlema. Eriti kui on inimene, kelle puhul ma arvaks, et ta on sama adekvaatne või kompetentne digiteemadel [nagu mina]. Ja kui tal midagi juhtuks, siis ma ütleks küll, et oi-oi, et äkki see, mis ma ikkagi praegu teen, ei ole piisav, et peaks võib-olla midagi rohkemat tegema.

37-aastane intervjueeritav

Need apsakad ja pettused... kui konkreetne [pettus] jõuab kellegi lähedaseni, eks need ju panevad asja reaalsemana nägema, et ei ole kuskil kaugel ja suvaliselt, vaid igapäevaelus, et sinuga võib juhtuda. Aga ega keegi ei reageeri enne, kui ukse taha ei tule see oht.

55-aastane intervjueeritav

Intervjueeritud PPA esindaja tunnistas samuti, et küberintsidendid inimese tutvusringkonnas ehk ehmatavad kogemuslood ja vahetu kontakt ohvriga on inimeste käitumise muutmisel mõjusamad kui üldine hoiatamine, sest need panevad inimest ohtu rohkem teadvustama. Ka intervjueeritud ITL-i esindaja kinnitas, et inimestele mõjuvad reaalelulised lood, millega saab end seostada ning õpitakse kõige paremini just endasarnastelt ja inimeselt inimesele leviva info kaudu.

Pikas perspektiivis inimesi oma käitumist muutma ei pane kindlasti see hoiatamine [et nt hoiatad meedias petuskeemide osas]. Rohkem sellised ehmatavad lood, vahetumad kontaktid inimestega – need on need kohad, kus inimesed rohkem enda jaoks teadvustavad seda ohtu.

PPA esindaja

Üks keskmise (35–44-aastaste) vanuserühma esindaja leidis, et ka üldisemalt küberturvalisuse teemasid, mitte ainult reaalseid juhtumeid, peaks esile tooma keegi, kes on inimese jaoks sümpaatne, lähedane ja autoriteetne. Kui teemast räägib oma võrgustiku või kogukonna liige, siis see võiks inimesi motiveerida rohkem teemale pühendumisele. Teine sama vanuserühma intervjueeritav märkis, et teda ongi varasemalt küberturvalisusele pannud tähelepanu pöörama sädeinimesest IT-meest, kes oli hästi pühendunud ning lähenes kolleegidele personaalselt ja hoolivalt.

Paljud intervjueeritavad nõustusid, et ka **võõraste kogemuslugude** kuulmine paneb teemale mõtlema ning on väärtuslikuks õppetunniks. Nende kogemuslugude jagamisega (nt

massimeedias) saab hoiatavate näidete abil kasvatada inimeste teadlikkust. Üks intervjueeritav nentis, et teema aktuaalsus meedias toob selle vaimses mõttes lähemale.

/.../ hirmutamise näited [motiveerivad tähelepanu pöörama], sest need tõesti jäävad meelde /.../ Päriselu juhtumid, mida kajastatakse meedias, need tõstavad kindlasti seda teadlikkust kuidagi. Tähelepanu sellele teemale, et kui keegi kaaseestlane ikka kaotas suure summa raha või mingi muu halb asi juhtus temaga internetis, siis läheb korda inimestele.

21-aastane intervjueeritav

/.../ [rohkem tähelepanu paneks pöörama] meedias mingid sellised lood, kus on keegi saanud kõrvetada. Jah, reaalsed näited. /.../ sellise materjali ma kindlasti loeks läbi, kui see oleks näiteks Eesti Ekspressis.

62-aastane intervjueeritav

Seejuures tõi paar intervjueeritavat välja, et rohkem tähelepanu panevad teemale pöörama just sellised kogemuslood, millega saab ise samastuda ja mille ohud on inimesele isiklikult lähedased. Üks intervjueeritav nentis tabavalt, et inimesed arvavad, et kui miski nendega juhtub, siis see on olude kokkulangemise tõttu, aga kui see kellegi teisega juhtub, siis see on sellepärast, et see keegi teine ei osanud paremini käituda. Küberturvalisuse vastu huvi tekitamiseks on seega oluline, et inimene kuuleks teemaga seoses endasugustest inimestest ja tunneks ennast nende lugudes ära. Vajadus kuulda eakaaslaste lugusid tõusis eriti esile noorimas (16–24-aastaste) vanuserühmas. Üks intervjueeritav pidas lisaks oluliseks, et esitatavad lood oleksid ajakohased (nt hetkel levivatest petuskeemidest), sest vana info ei tekita tunnet, et ohud on endiselt aktuaalsed.

/.../ ma alati pensionäride kohta loen, aga nendega ma ka ei samastu, sest ma usun, et ma 30 000 eurot siiski kellelegi üle ei kannan. /.../ Aga neid lugusid, mis räägivad natuke minu jaoks tõenäolisematest ohtudest, mis on seotud paroolide ja *account hijack* imistega [konto kaaperdamistega] – mis on rohkem Google, Facebook ja niimoodi – nende kohta ma tegelikult kuulen üpris vähe. Kui need lood selle kohta räägiksid, siis see paneks [rohkem tähelepanu pöörama].

37-aastane intervjueeritav

Teistele eeskujuks olemine ning eduelamuse saamine

Intervjueeritud küberturvalisuse ekspert märkis, et küberkäitumise mõjutamisel võib toimida see, **kui inimene peab teisi õpetama ja olema oma käitumisega teistele eeskujuks**, mis läbi muudab ta ka enda praktikaid:

Inimene muudab käitumist siis, kui ta satub positsiooni, kus ta peab teistele nõu andma ja ta peab teistele eeskujuks olema /.../ Kui me aitame inimestel võtta vastutust, mõista seda ja seda [teadmist] jagada teistele, et see ongi sinu ülesanne nüüd aidata teisi, kes on sinust nõrgemad; jälgida oma vanemaid ja aidata oma vanavanemaid – siis need inimesed võtavadki selle vastutuse.

küberturvalisuse ekspert

Üks keskmise (35–44-aastaste) vanuserühma esindaja tõdes, et **eduelamus** võib olla oluline motivaator küberturvalise käitumise juurutamisel. Ta tõdes, et tema peal töötaks lihtne ja edu rõhutav sõnum, nt „suurepärase asi, tee seda!“ või „neli lihtsat sammu“, mis tekitaks tal hea tunde, kui ta need ära teeb ning paneks end pädevana tundma. Tema hinnangul on vaja tekitada inimestes n-ö digioptimismi ehk tunnet, et saab midagi kerget ja praktilist teha, mis päriselt loeb.

Lisaks leidis üks noorema eagrupi intervjuueeritav, et inimesed, kes teavitavad vastavaid instantse (nt PPA-d või RIA-t) küberohtudest (nt petuskeemist, õngitsuskirjast, kahtlasest veebilehest) võiksid saada tagasisidet, kas nende teavitus läks läbi ja kas probleemiga on tegeletud. Tema hinnangul võiks inimesi tänada, kui nende abil midagi avastatakse või lahendatakse, sest see tekitaks teavitajas hea tunde, et ta aitas kaasa interneti turvalisemaks tegemisele, mis omakorda innustaks küberturvalisusele veelgi enam tähelepanu pöörama. Rõhutame, et PPA varem juba ka rakendanud avalikkuses inimeste tänamist kui küberturvalisusele positiivse sõnumiga lähenemise meetet (vt lähemalt ptk 1.1).

3.3.2. Välised motivaatorid

Materiaalsed stiimulid, sh auhinnad ja preemiad

Uurisime intervjuudel muuhulgas, kas materiaalsed stiimulid nagu rahalised preemiad ja allahindlused või auhinnad, võiksid innustada inimesi küberturvalisusele rohkem tähelepanu pöörama.

Intervjuueeritavad tõdesid, et **materiaalsed preemiad võiksid nende hinnangul küll innustada inimesi küberturvalisusele rohkem tähelepanu pöörama**. Nii mõnigi intervjuueeritav kinnitas, et teda isiklikult või inimesi üldisemalt (kes muidu ei pruugi küberturvalisusele mõelda) motiveeriks oma ohutuse nimel rohkem tegutsema millegi vastu saamine. Üks intervjuueeritav tõi näitena analoogi veebikaubandusest: on ju e-poodideski tihti pakkumine, et liitudes uudiskirjaga saab järgmiselt ostult allahindlust. Olgugi et kõik seda võimalust enamasti ei kasuta ega soovi saada liigselt (reklaam)kirju, võiks mingile grupile elanikkonnast selline lähenemine siiski hästi sobida ka küberturvalisuse kontekstis.

Kui saada auhind lihtsalt selle eest, et ei pannud enda täisnime kuskile saidile, siis see on nagu – no problem [pole probleemi]! Andke see kingitus mulle siis niisama. Ma ei tea, kuidas nad seda kontrolliks. Aga muidu – pole halb mõte.

16-aastane intervjueeritav

Kui on mingid kampaaniad või asjad, et koolita oma vanem ja saad kinkekaardi või midagi sellist, [siis see motiveeriks rohkem tähelepanu pöörama].

39-aastane intervjueeritav

/.../ see ei pea olema rahaline motivatsioon, aga see võib olla mingi soodsama teenuse saamine näiteks. /.../ Sellises hapras olukorras nagu me oleme, kus me peame mõtlema igapäevasele leivale juba praktiliselt, et ma arvan, et see /.../ lähiaastatel muutub veel olulisemaks, et inimene muu mure kõrvalt mõtleb ka sellele turvalisusele tänu sellele, et ta saab näiteks mingisuguse konkreetse teenuse või toote soodsamalt.

58-aastane intervjueeritav

Paar intervjueeritavat seostasid materiaalseste stiimulite kasutamisega inimeste motiveerimisel ka mängustamise potentsiaali. Nende silmis võiks turvalisuse hoidmine olla mänguline: midagi tuleb teha selleks, et auhinda saada. Üks neist arvas seejuures, et selline lähenemine sobiks hästi just nende inimeste puhul, kelle teadlikkus ongi madalam ja kes osalevad samas sageli niikunii erinevates (kohati kaheldava turvalisusega) e-mängudes, kampaaniates jms.

Ma arvan, et pigem see [rahaline preemia] mõjutaks küll. Kui turvalisuse hoidmine muutuks mängulisemaks või oleks sihuke *gamefication* [mängustamine], et teed mingid sammud ära ja siis sellega kaasneb mingisugune kinkekaart või soodustus või midagi sellist.

37-aastane intervjueeritav

Samas rõhutasid mitmed intervjueeritavad, et **sellisel mängulisel premeerival lähenemisel on ka piiranguid ja riske**. Nt tõid nad välja usalduse puudumise sellise meetodi suhtes, sest auhinnad ja rahalised stiimulid seostuvad sageli kelmustega, mis võib tekitada inimestes ettevaatlikkust või isegi skepsist. Rahalise preemia kohta nt sõnumi saamine võib panna inimesi kahtlema, kas tegu on omaette pettusega. Paar intervjueeritavat nentiski, et sellist lähenemist võivad ära kasutada petturid inimeste andmete kätte saamiseks, esitledes ennast nt ametlike teenusepakkujatena.

Ma arvan, et kuna see teema on niisugune, kus öeldakse, et kõik ei ole kuld, mis hiilgab, siis see võib-olla tekitab seda vastureaktsiooni just, et okei, ma saan auhinna selle eest, kui ma olen veebiteadlik, aga samas hästi paljude kelmustega käivad kaasas ka mingid auhinnamängud.

24-aastane intervjuueeritav

Lisaks mainis osa intervjuueeritavaid, et väline stiimul ei pruugi viia tegeliku käitumismuutuse, kui preemia nimel täidetakse vaid formaalsed nõuded (nt vahetatakse lihtsalt parool ära või tehakse preemia saamiseks koguni lisakonto), ilma et teadlikkus tegelikult suureneks või küberturvalisusele püsivalt rohkem tähelepanu pöörataks. Tegutsemisele ergutavate stiimulite kõrval on oluline siiski inimese sisemine motivatsioon oma turvalisust tagada.

/.../ siis on jällegi see häda, et neid [küberturbepraktikaid] hakataksegi tegema just selle preemia pärast. Näiteks kui see parooli vahetamine – vaadatakse, et okei, ma pean lihtsalt parooli ära vahetama – aga võib-olla ei vaadata, kas see parool on näiteks turvaline või kas ma olen seda kusagil varem kasutanud.

Lihtsalt tahetaksegi seda preemiat saada.

18-aastane intervjuueeritav

Kui inimene ise ei ole endale teadvustanud, et turvalisus on oluline, siis mingi rahaline boonus või kinkekaart... ma ei tea. /.../ see paneb korraks võib-olla mõtlema sellele [küberturvalisuse olulisusele].

59-aastane intervjuueeritav

Kampaaniad, meeldetuletused ja reklaamid

Osa intervjuueeritavate sõnul on motiveerivad **avalikud kampaaniad ja meeldetuletused**. Nad peavad neid mõjusaks, sest need tõmbavad teemale tähelepanu ja toovad selle korraks fookusesse, mis paneb inimesi (kasvõi korraks) teemale mõtlema, tõstes seeläbi ehk ka teadlikkust. Üks keskmise (35–44-aastaste) vanuserühma esindaja tõdes, et ka automaatsed meeldetuletused (nt paroolihaldaja poolt saadetud meeldetuletus oma salasõnu uuendada või sotsiaalmeedia rakenduses ette tulev teade) motiveerivad tõenäoliselt küberturvalisusele rohkem tähelepanu pöörama.

Üks vanima (55–64-aastaste) vanuserühma esindaja rõhutas, et küberturvalisusele paneb rohkem tähelepanu pöörama **sõnumite pidev kordamine**. Tema arvates võiks nt meedia veebilehtedel aeg-ajalt joosta teemakohased reklaamid. Küberturvalisusalase info kordamist avalikkuses on käsitletud eelpool peatükis 3.2, mis avab nii selle poolt argumente kui soovitud vastupidist mõju ning kirjeldab Eesti elanike vastakaid tundeid sõnumite pideva kordamise osas.

3.4. Kuidas võiks inimeste küberteadlikkust ja -käitumist edendada?

Selleks, et inimeste küberteadlikkust ja -käitumist edendada, tuleb välja selgitada tõhusad ja sihtrühmadele vastuvõetavad käitumise mõjutamise viisid. Seetõttu küsisime uuringu käigus intervjueeritavate muuhulgas seda, milliseid kanaleid, formaate ja tegevusi võiks nende meelest kasutada, et teema inimeste teadvusesse viia ning neid küberturvalisemalt käituma mõjutada. Samuti uurisime, millistest sõnumitest ja kõneisikutest võiks olla intervjueeritavate hinnangul kasu küberturvalisusega seotud info kommunikeerimisel.

3.4.1. Milliseid kanaleid/formaate/tegevusi võiks kasutada?

Anname järgnevalt ülevaate intervjueeritavate poolt välja toodud potentsiaalikest kanalitest/formaatidest/tegevustest, eristades neid seejuures vastavalt sellele, 1) kas tegu on kanalite/formaatide/tegevustega, mida Eestis küberturvalisuse edendamisel juba rakendatakse või on rakendatud, või 2) kas tegu on uute või ka senisest süsteemsemalt rakendamist vajavate kanalite/formaatide/tegevustega. Arvestades, et meil puudub täielik ülevaade sellest, mida on kõikjal üle Eesti, kasvõi üksikutes asutustes või väikese sihtrühmadega, küberturvalise käitumise edendamiseks tehtud, lähtume siinkohal eelkõige infost, mida käsitlesime ka peatükis 1.1, kus andsime ülevaate küberturvalise käitumise edendamisega seotud osapooltest ja nende senisest tegevusest.

KANALID/FORMAADID/TEGEVUSED, MIDA RAKENDATAKSE VÕI ON RAKENDATUD

Massimeedia, sotsiaalmeedia ja avalikud teavituskampaaniad

Mitmed intervjueeritavad (eeskätt keskmisest ja vanemast eagrupist) mainisid, et see, kui infot küberturvalisuse teemal jagatakse massimeedias, pälvib nende tähelepanu. Nt pakkusid nad, et **ajalehtedes ja suuremates uudisteportaalides** võiks jätkuvalt jagada teiste inimeste õpetlikke kogemuslugusid. Ühtlasi tõdes üks intervjueeritavatest, et veebiväljaannetes on sellised lood sageli maksumüüri taga, piirates inimeste ligipääsu harivale infole, mis tähendab, et sellele takistusele tuleb mõelda või siis jagada kogemuslugusid nt hoopis avalike kampaaniate formaadis.

Üks vanema eagrupi intervjueeritavatest pakkus muuhulgas, et üks kanal, mille kaudu võiks küberturvalisusalane info jõuda päris paljude inimesteni, on **kohalikud lehed**.

Lisaks kirjutavale meediale tõtsid eri vanuses intervjueeritavad esile ka **televisiooni** kui infokanali olulisust, kuid ka sel puhul on oluline mõelda, millises võtmes küberturvalisuse teemat täpselt käsitleda. Lühikestest reklaamklippidest enam näeksid intervjueeritavad väärtust teemakohastes telesaadetes või ka selles, kui küberohtude teema põimitaks kuidagi mõne telesarja (nagu „Õnne 13“ või vahepeal noorte seas väga populaarne olnud

„Kättemaksukontor“) sissusse. Samuti töid nii intervjueritud küberturvalisuse ekspert kui ka ITL-i esindaja välja telesarjad kui perspektiivika viisi inimestele küberturvalisusalast infot jagada. Viimane neist nimetas sarnaselt ühele nooremaste vanuserühma kuulunud intervjueritavale ühe sobiliku teleformaadina ka populaarteaduslikke saateid nagu „Rakett 69“.

Miks mitte mingisugune saatesari. Näiteks nagu teaduste populariseerimiseks Rakett69 on tegelikult päris palju seda [teema populaarsust] tõstnud.
24-aastane intervjueritav

Erinevaid küberturvalisusalaseid avalikke kampaaniad on toimunud mitmesuguseid ja intervjuude põhjal võib öelda, et paljud inimesed näevad neis endiselt perspektiivikat viisi, kuidas teema olulisust esile tõsta. Nt tões üks 58-aastane intervjueritav, et tema meelest toimivad kampaaniad väga hea meeldetuletusena. Keskmises eagrupid mainisid paar intervjueritavat, et neid innustaks küberturvalisusega tegelema kampaania, mis on kuidagi kiiksuga või humoorikas:

Väga hea nali või kampaania, mis kutsub tegutsema, aga teeb nalja – see paneks mind kaasa lööma või tõmbaks tugevalt.
37-aastane intervjueritav

Lisaks massimeediale töid mitmed eri vanuses intervjueritavad küberturvalise käitumise edendamisel välja ka **sotsiaalmeedia** rolli. Leidus üsna palju intervjueritavaid, kes leidsid, et (eeskätt noorema publiku kõnetamiseks) oleks kasu erinevatest lühivideotest, mis lihtsal moel küberturvalisuse põhitõdesid selgitaksid ning meelde tuletaksid.

Võib-olla olekski kasu sellest, et mingid eestikeelsed videod, sellised lühemad... Kui TikTakis tuleks midagi sellist huvitavat ette, kuidas need skämmerid [petturid] üldse saavad su numbri kätte, siis ma vaataks selle läbi.
16-aastane intervjueritav

Mina kui noor tegelikult väga armastan lühiformaati /.../ Ma olen ka näinud mingeid [küberturvalisusteemalisi] klippe ja ma ise väga hea meelega tarbin [neid]. Et kui mingid nooremad sisuloojad näiteks teeksid Instagrami või TikToki selliseid informatiivseid videoid, see kindlasti oleks väga toetav minu arvates.
23-aastane intervjueritav

Sellised väikesed videoklipid, kus tõesti on tekst ja visuaal ilusasti kokku pandud, on vajalikud.
59-aastane intervjueritav

Koolitused

Keskmise ja vanema eagrupi intervjueeritavad tõid mõnel korral välja, et rohkem võiks toimuda ka küberturvalisusalaseid koolitusi. Seejuures tõdesid nad, et koolitused on formaat, mis sageli sobib just **vanemate inimeste teadlikkuse ja oskuste arendamiseks**. Üks 58-aastane intervjueeritav tunnistas, et talle meeldivad koolitused just vahetu kontakti tõttu: koolitajat saab kohe segaseks jäänud nüansside kohta lisa küsida ning paluda konkreetseid näiteid.

Kui ta [koolitaja] näitabki sulle näiteks kahte pilti kõrvuti, et üks on nüüd see niinimetatud valekraan, teine on see õige. Minu jaoks vahetu kontakt on muidugi parem, see jääb paremini meelde. Ja siis kui sa saad küsida veel üle... Kui sa [küberturvalisusalase] klipi vaatad ära – kui ei saanud aru, ei saanud aru, eks ju. Aga kui saad küsida kohe [koolitajalt] – see mulle väga meeldis.

58-aastane intervjueeritav

Mõned keskmise eagrupi intervjueeritavad leidsid, et kui koolitusi korraldada, peaksid need olema mitte loengu stiilis, vaid **info edastamine võiks toimuda eluliselt, kaasavalt ja interaktiivselt**.

[Koolitustel] näidisolukordade läbimängimine näiteks [oleks hea]. See käivitab inimese kaasamõtleme, empaatia, see paneb teda süvenema. /.../ Et see [koolitus] ei kujune selliseks loenguks, kus tark inimene räägib, näitab slaidide pealt ja siis teised teesklevad õppimist ja kuulamist, aga midagi aru ei saa. See võiks ikka väga interaktiivne olla /.../

44-aastane intervjueeritav

Pakutavate koolituste puhul on seejuures oluline arvestada, et need võiksid olla **tasuta**, et tagada ligipääs võimalikult paljudele huvilistele. Ka üks intervjueeritav tõdes, et ta on küll küberturvalisusalastel koolitustel osalenud, kuid teeks seda tasuta meeleldi veelgi:

/.../ [küberturvalisuse] algkoolituse ma käisin läbi ja siis natuke edasijõudnutele /.../ Ma tahaks veel ikkagi, mis vähegi tasuta on kursusi.

58-aastane intervjueeritav

Samuti on koolituste puhul oluline mõelda, kuidas võiks end harima meelitada ka need inimesed, kes küberturvalisusest eriti ei huvitu, kuid küberturbe põhitõdede tundma õppimist tegelikult väga vajaksid. Üks intervjueeritavatest viitas nt võimalusele läheneda mitteformaalse hariduse osas kogukondlikult, **kasutades inimeste õppima innustamiseks kogukonnas autoriteetseid isikuid**.

Küberturvalisusalane harimine koostöös tööandjatega

Nagu ka peatükis 1.1 välja tõime, üritab PPA juba praegu teha koostööd tööandjatega, et nende kaudu tööealise elanikkonnani jõuda ning seeläbi inimeste küberteadlikkust edendada. Ühtlasi, nagu eelnevates peatükkides (vt ptk-d 2.5.1 ja 3.1) kirjeldasime, on töökoht inimeste jaoks sageli üks infoallikas küberturvalisusalase teabe saamiseks ning see, kui töökohal on küberturbe põhitõdede järgimine ja turvaliste praktikate rakendamine kohustuslik, paneb inimesi ka oma küberkäitumist rohkem jälgima. Nii tõdesid mitmed intervjueeritava, et neile tundub inimeste küberturvalisusalane harimine koostöös tööandjatega mõjus ja nutikas viis, mida võiks rakendada laialdasemalt.

Seejuures leidsid nad, et kui ettevõtetega koostöös korraldada koolitusi ka neile töötajatele, kelle töö ei hõlma digivahendite kasutamist, oleks tõenäoliselt võimalik jõuda ka nende inimesteni, kes on digikaugemad ning vähemate teadmiste- oskustega. Just seetõttu pidasid intervjueeritavad koostööd tööandjatega ka perspektiivikaks viisiks, kuidas inimeste küberteadlikkust ja -käitumist edendada.

Ma arvan, et kõige lihtsam võiks olla [inimesteni jõuda] ikkagi läbi töökohtade. Minu meelest võiks olla suurtes töökohtades, suuretevõtetes oluliselt tugevam IT-turvalisuse koolitus kõikidele töötajatele. See algab sellest, et ettevõtte enda infosüsteemid on tänu sellele turvatud. Aga tegelikult peaks see olema nii, et koristajast direktorini infotund, et kuidas elimineerida või minimeerida see oht seal tooli ja klaviatuuri vahel. /.../ Lõpuks saadakse [töökoha kaudu] kätte see inimene, kes käib kaks korda kuus oma netipangas ja meile vaatamas. Temani on vaja jõuda mingisuguse füüsilise kanali kaudu, mis ei ole internetis.

39-aastane intervjueeritav

Kindlasti oleks [kasulik inimesteni üritada jõuda tööandjate kaudu]. /.../ Üks asi on tööandja pool, mida ta ettevõttes peab oma andmete ja IT-parkide jaoks tegema, aga just see, et mida inimene saab teha, kuidas tema enda kontod ja elementaarsemad asjad seal /.../ Elementaarne oskus: kui palju sa saad ID-kaardi kasutuse turvalisemaks muuta; kuidas sa saad iseenda andmeid ja oma kontosid kaitsta, kõik selline. Selline standardne turvalisus, mille vastu tihti ikkagi eksitakse.

59-aastane intervjueeritav

Lisaks mainis üks vanema eagrupi intervjueeritav, et kuigi ta oli kunagi töökohal tehtavate digioskuste testide osas skeptiline, leiab ta nüüd, et neid teste tuleks teha rohkem, et inimeste valvsust ülal hoida.

Kui alguses need [digioskuste] testid [tulid], võib-olla 10 aastat tagasi või millal ma hakkasin testima... mulle tundus ta [testimine] hästi mõttetu. Ma tõesti suhtusin sellesse, et „no mida iganes“. Aga mida aasta edasi, seda rohkem ma saan aru, et tegelikult võiks selline test olla ka näiteks koolilastele ja ma olen küsinud, kes töötavad teistes asutustes, et [neil] ei ole testimist. Võiks olla.

58-aastane intervjueritav

KANALID/FORMAADID/TEGEVUSED, MIS ON UUED VÕI VAJAKSID SENISEST SÜSTEEMSEMAT RAKENDAMIST

Personaalne või väikestes gruppides nõustamine

Kõikide eagruppide intervjuerivate seas leidus neid, kes olid arvamusel, et senisest palju enam võiks inimestele küberturvalisuse teemal pakkuda personaalset nõustamist. Paar noorema vanuserühma intervjueritavat pakkusid välja, et olemas võiks olla küberturvalisuse **infotelefon või veebipõhine platvorm** (nt foorum), kust igal ajal saaks nõu küsida.

Mina olen väga tugev infotelefonide kasutaja. Kui mul on mingi küsimus näiteks maksu teemadel, siis ma alati helistan [Maksu]ameti infotelefonile. Kui selline [küberturvalisuse infotelefoni] võimalus on, siis ma oleksin kindlasti see, kes helistab ja personaalsetele küsimustele vastuseid soovib.

24-aastane intervjueritav

Tuletame siinkohal meelde, et nagu ka peatükis 1.1 välja tõime, on RIA poolt varem töös olnud venekeelsele elanikkonnale suunatud infoliin, kuid tegu oli kitsalt sihtrühmale mõeldud kanaliga, mida võiks tegelikult rakendada (või vähemalt piloteerida) ka laiemas kasutajaskonnas.

Vanema eagrupi intervjueritavatest peavad samuti paljud personaalset lähenemist väga tähtsaks ja just eakatele inimestele sobivaimaks. Personaalsust kas siis päris individuaalse nõustamise või ka väikeste töötubade/õpiringide formaadis peavad intervjueritavad oluliseks nii seetõttu, et eakamate inimeste digioskuste tase on väga varieeruv, aga ka sellepärast, et personaalne või väikeses grupis nõustamine, mitte suurem koolitus, võimaldab teemat selgitada aeglasemalt ja seeläbi inimesele arusaadavamalt.

Ma usun, et see [personaalne lähenemine] on asja võti, et kuskile kohale jõuda.

Tuleb suhelda nendele [vanemaealistele] arusaadavas keeles ja viisil. /.../

Kõigepealt peab endale selgeks tegema, mis tase kellelgi on. Ja siis vastavalt edasi minema selle baasil.

64-aastane intervjueritav

Väga paljud [eakamad inimesed] on [raamatukogusse] tulnud ja öelnud, et nad on küll käinud ka [digioskuste/küberturvalisuse] grupikoolitustel, [aga] et seal räägitakse nii kiiresti, nad ei saa aru sellest. Nad jäävad maha ja lõpptulemusena ega nad sealt [koolitusest] ei saagi midagi.

58-aastane intervjuueritav

Ühtlasi võimaldaks niisugune lähenemine õppimise käigus selguvates keerulisemates kohtades individuaalset tuge saada ja tagaks inimese pädevuste pideva arengu, kuna teadmisi-oskusi ei omandataks mitte passiivselt kuulates, vaid ise aktiivselt katsetades ja „pusides“.

Üks 64-aastane intervjuueritav kirjeldas muuhulgas seda, kuidas ta on pikkamisi arendanud oma 80. eluaastates naabrimehe digioskusi. Selle kogemuse põhjal tõdes ta, et vanemate inimeste õpetamine ja nende küberteadlikkuse ning -oskuste edendamine on aeganõudev ning nõuabki väga selgelt ja elulist lähenemist:

Mõned aastad tagasi, kui ma kolisin, siis mul naabrimeheks sattus kaheksakümneaastane papi, kes väga vaevaliselt vaatas [digiseadmeid], aga ega ta suurt midagi aru ei saanud. Ja poole aastaga tegin tast päris vinge internetis surfaja. /.../ Seda tüüpi [eakatel digimaailmast kaugetel] inimestel tuleb asi võimalikult lihtsaks teha. /.../ Kui näiteks lähed Facebooki, [siis selgitada] mis on pealeht ja mis on tema oma leht – kuidas seal ringi surfad, [seda] tuleb talle seletada. Mina seletasin näiteks niimoodi, et Facebook: kui sa sinna sisse logid, et see on nüüd „kopp-kopp, ma olen nüüd oma kodus“. Ja nüüd vot siit lähme sinna tuppa, kus asuvad need asjad, ja sealt lähme sinna tuppa, kus asuvad need asjad. Võimalikult lihtsalt [asjad] selgeks teha nendele arusaadavas keeles.

64-aastane intervjuueritav

Üks raamatukogus töötav intervjuueritav tõi personaalse lähenemise plussina välja ka selle, et kui eakad tulevad personaalsele nõustamisele konkreetse küsimuse või murega, siis tegelikult saab neile selgituste käigus jagada ka laiemat küberturvalisusalast teadmist ning nügida inimesi turvalisemalt käituma:

Meil raamatukogus on, et on võimalik tulla [digioskuste osas] abi saama /.../ Aga seal nad [vanemad inimesed] ei tule mitte selle küsimusega, et kuidas nüüd olla [küber]turvaline, vaid nad lihtsalt ei oska [digiseadmetes/internetis toimetada] – kuidas ma teen nüüd seda ja kuidas ma teen toda. Selle [nõustamise] käigus me räägime neile turvalisusest. Aga mitte ükski [vanem inimene] pole tulnud, et „Vot, nüüd tahan olla [küber]turvaline!“. Sellist otsust lähenemist [küberturvalisusele] ei ole ja ei selle peale ei tule keegi kohalegi ise /.../ Aga kui on abivajamine, siis see [lisaks küberturvalisusest üldisemalt rääkimine] on selline kaudne nügimine. Et „Sa nüüd tahad hakata seda [seadet/rakendust] kasutama, aga vaata selle juures nüüd ka seda [mõnd muud olulist aspekti].

62-aastane intervjueritav

Oluline on siinkohal meeles pidada, et nagu ka eelmisest tsitaadist näha, teevadki raamatukogud juba pikka aega tänuväärset tööd (sh pakkudes personaalset nõustamist) inimeste juhendamisel, et nende pädevused erinevate digiteenuste ja digiseadmete kasutamiseks oleksid piisavad. 2022. aastal ilmunud uuringu „Rahvaraamatukogude rolli analüüs ja ettepanekud valdkondadevahelise koostöö tõhustamiseks“ (Murasov jt, 2022) tulemuste järgi on koguni 85% uuringu raames toimunud küsitlusele vastanud rahvaraamatukogudest pakkunud elanikele tuge e-riigiga seotud digitoimingutes. Samuti on nimetatud uuringus välja toodud, et enamasti vajavad raamatukogude külastajad tulenevalt erinevatest vajadustest ja eri tasemel teadmistest-oskustest just individuaalset juhendamist. Ka RIA on varasemalt vanemaealistele suunatud küberturvalisuse õpitube korraldanud ning nende raames on olnud võimalik osalejatel ise küsimusi esitada ning just oma muredega seoses nõu paluda, kuid võib järeldada, et nõudlus sellise personaalse lähenemise vastu on märksa suurem, kui ainuüksi niigi ressursipuuduses vaevlevad rahvaraamatukogud või RIA üksikute töötubade abil suudavad rahuldada.

Küberturvalisuse edendamise süsteemne lõimimine haridusasutuste tegevustesse

Nagu peatükis 1.2 tõdesime, puudub laste ja noorte küberteadlikkuse arendamise puhul süsteemne valdkondadeülene lähenemine ning olgugi et haridusasutustel on teema vastu huvi, pole seni õnnestunud riikliku visiooni puudumisel küberturvalisuse edendamist ka süsteemselt haridusasutuste tegevustesse lõimida. Noorema vanusegrupi intervjueritavad töid küll (kõrg)kooli välja ühe infoallikana, kust nad küberturvalisusalaseid teadmisi saavad või on saanud, ent korduvalt tõstsid nii intervjueritud eksperdid kui tavainimesed (kõrg)koolide kaudu küberturvalisuse edendamist esile perspektiivika lähenemisena, mida võiks veelgi rohkem kasutada. Niisiis viitab seegi soov sellele, et küberturvalisuse edendamine haridussüsteemi kaudu peaks olema süsteemsem ja haridusasutustes tuleks kasutada senisest mitmekesisemaid formaate ning tegevusi.

Nii mõnedki intervjueritavad tõdesid, et **küberturvalisus on teema, mis võiks olla rohkem eri moel õppetegevusse integreeritud**. Kui üks intervjueritavatest pakkus, et nii kõrg- kui

ülikoolides võiks kaaluda eraldi kohustusliku küberturvalisusteemalise kursuse/õppeaine loomist, siis sellest enam tõusetus intervjuudest idee, et küberturvalisuse teema peaks olema orgaaniliselt õppetegevustesse lõimitud. Seda tõdesid mõned noored, aga ka üks keskmise eagrupi intervjuueriv, kes tõi näite, kuidas tema meelest võiks **küberturvalisuse teemat rohkem käsitleda eri ainetundides:**

[Küberturvalisuse teema] võiks olla ka enam integreeritud erinevatesse koolitundidesse. Näiteks miks mitte õppidagi eesti keelt, aga on mingi interneti juhtum [loo teemaks] või midagi – harjutatakse lugemist seal, aga samas sellele järgneb arutelu, millest just juttu oli; kuidas niisugust juhtumit vältida või mida just seal [loos] keegi hästi tegi ja nii edasi. Või siis on, [et] tehakse matemaatikas mingi tekstülesanne /.../
41-aastane intervjuueritav

Noorema eagrupi intervjueeritavatest tunnistas üks inimene, et ta ei vaataks küberturvalisusalaseid õppevideosid, kui ta ei peaks, aga kui nende vaatamine oleks mõne õppeaine (nt informaatika) raames kohustuslik, siis oleks see viis, kuidas hariv materjal ikkagi noorteni jõuaks. Lisaks tegi üks 16-aastane intervjueeritav ettepaneku, et nii nagu eksisteerib programm „Liikuma kutsuv kool“, võiks mingi sarnane algatus (nt „Netiturvaline kool“ olemas olla ka küberturvalisuse teemaga seonduvalt.

Lisaks küberturvalisuse teema aineõppesse lõimimisele pakkusid nii intervjueeritud PPA esindaja kui ka paar noort formaatide mõttes välja, et võiks olemas olla hariv arvutimäng, mida saaks koolides kasutada ja selle abil laste ja noorte küberteadlikkust edendada.

[Õppemäng] oleks väga, väga hea idee. /.../ Ma kujutan ette, et lapsena, kui ma oleks mänginud midagi... Näiteks mingi programm: sul on virtuaalne postkast ja sulle saadetakse sõnumid ja siis sa klikkad need läbi, teed ise asju. Ja siis lõpuks [mäng] sulle ütleb, kui turvaliselt sa tegelikult käitusid ja kui sa oleks päriselus midagi sellist teinud, kas sa oleks saanud häki või mida peaks turvalisemalt tegema /.../ See oleks lapsele väga kasulik. /.../ [Oleks] turvaline mäng, aga [sa saaksid mängimise kaudu teada, et] kui see ei oleks mäng ja kui sa teeks niimoodi, mis võiks juhtuda sinu informatsiooniga.
16-aastane intervjueeritav

Peale arvutimängu tulid intervjuudel noortega jutuks ka **küberõppused ja -testid**, mida nad näevad mõjusa viisina küberturvalise käitumise edendamisel. Nt võiks reaalse ohusituatsiooni läbi mängimine aidata noorel paremini mõista, kuidas tuleks päriselus toimida ning milline on küberturvaline käitumine, mille poole püüelda:

/.../ korraldada koolides õppusi sel teemal, kus läbi mängida, et [mida teha] kui midagi on juhtunud /.../ Näiteks keegi on sulle [kontole] sisse hâkkinud ja sinu isikuandmed ja paroolid saadetakse sulle meiliga ja sa saad aru, et kellelgi teisel on see info. Mida järgmisena teha? Seda [edasisi olulisi tegevussamme] läbi teha mingi tunni või õppuse raames. Ma usun, [et see] aitaks paremini mõista tihti, mida see päriselt võib hõlmata, kui sind interneti kaudu rünnatakse ja mis oleks õige käitumine.

21-aastane intervjuueritav

Ühel noorema vanuserühma fookusrühma intervjuul tuli seoses noorte võimaliku võltsenesekindlusega ja oma küberteadmiste üle hindamisega jutuks ka nn **šokiteraapia**. Arutasime intervjuul osalejatega, kas kasu võiks olla sellest, kui haridusasutustes leiaksid aset nt küberturvalisuse kuud või nädalad, et esmalt inimeste tähelepanu teemale tõmmata, ning seejärel mingi aeg hiljem toimuks (kõrg)koolis küberturvalisusalase valmisoleku testimine nii, et õppijaid sellest ette ei hoiatataks. Nt saadetakse haridusasutuse IT-osakonna abiga tudengitele kõrgkooli meilile fabritseeritud petukiri või palutaks üldhariduskooli õpilastel klikkida eKoolis või Stuudiumis mõnele lingile. Erinevalt tavalisest IT-testist, kus inimene keskendub testi tehes tõenäoliselt rohkem ja on oma tähelepanu spetsiaalselt suunanud ohukohtade tuvastamisele, võiks eelkirjeldatud lähenemine mõjutada inimesi nende igapäevarütmis. Haridusasutused saaksid üheltpoolt ülevaate, kui paljud õppijad sellise testi raames ikkagi läbi kukuvad ja kui palju tuleks küberturvalise käitumise edendamisele veel tähelepanu pöörata, noored ise aga saaksid testis õnnestudes või ebaõnnestudes tagasisidet oma tähelepanelikkuse (või selle puudumise) kohta. Nii oleks ehk võimalik muuta olukorda, kus noored arvavad, et nendega ei juhtu kübermaailmas niikuinii midagi, ning motiveerida neid edaspidi (veelgi) küberturvalisemalt käituma.

See [eelkirjeldatud šokiteraapia stiilis lähenemine] võiks täitsa olla *wake-up* [äratuskell] ka paljudele inimestele tegelikult. /.../ Sa näed oma teo tagajärgi ja sa oled, et "Oota, mis ma nüüd siis valesti siin tegin? Kuidas see nii on?".

24-aastane intervjuueritav

Ühest küljest meil on ju nii normaalne, et meil on tuletõrjeõppused näiteks, mida koolides tehakse ka. Miks siis ei võiks olla nii, et meil on ka sama regulaarselt – näiteks iga aasta erinevatel aegadel – sellised võimalikult tõetruud või siis vähemasti reaalsuse lähedased testid.

24-aastane intervjuueritav

Testisime seda ideed hiljem ka ühe keskmise eagrupi fookusrühmaintervjuul, kus osalejad arvasid samuti, et sellisest tegevusest võiks olla kasu ning nii-öelda turvaline ohukogemus võiks panna noori ja tegelikult ka laiemalt kõiki inimesi oma küberkäitumise peale järele mõtlema.

Küberturvalist käitumist toetavate tehnoloogiliste lahenduste ja meeldetuletuste kasutamine

Kirjeldasime peatükis 2.5.1, kuidas inimesi ajendab küberturvaliselt käituma see, kui tehnilised lahendused (nt teatud kohustuslikud sätted, automaatsed hoiatused/meeldetuletused) nügivad neid ohutusele tähelepanu pöörama. Seda, et toetavaid tehnoloogilisi lahendusi ja meeldetuletusi võiks küberturvalisuse edendamiseks veelgi ulatuslikumalt ja süsteemsemalt rakendada, pakkusid välja mitmed intervjueeritavad (eeskätt keskmisest eagrupist).

Üks intervjueeritav nimetas ühe võimalusena seda, et võiks leiduda lahendus, mis nt mõnel veebilehel uut kontot luues kohe automaatselt kontrolliks, kas isiku meiliaadress, millega ta kontot teha tahab, on juba varem olnud osaline andmelekkes. Selline lähenemine võiks juhtida inimeste tähelepanu võimalikule ohule ega eeldaks samas, et inimesed ise andmelekete kohta uurivad, vaid viiks hoiatuse otse kohale ka vähem valvsatele.

Samuti tõi sama intervjueeritav välja, et kui toimunud on mõni suurem andmeleke, võiks teavitust selle kohta tulla riigilt (nt eesti.ee vahendusel) kui usaldusväärset allikalt. Selline viis oleks tema hinnangul eriti kasulik, sest iga inimene ei pruugi teada, kust kaudu saab oma andmete lekkimist kontrollida, ning isegi kui ta on sellega kursis, ei pruugi ta seda sammu astuda, et kontroll ära teha.

Kui oleks riigipoolne mingisugune [teavitust]. Et riik saadab läbi eesti.ee mulle kirja, et „Tere, teie info on lekkinud selle veebilehe andmetel. Palun jälgige, et te ei kasuta kuskil sama parooli.“. Et näiteks Dropboxis [paroolid] lekkisid. Kui riik saadaks mulle [sellise teavituse], siis ma võtaks seda veel tõsisemalt, kui et ma läheks ise seda kontrollima kuskile. Paljud võib-olla ei teagi, kust kontrollida.

39-aastane intervjueeritav

Nooremast vanuserühmast leidis üks intervjueeritav muuhulgas, et see, kuidas Mobiil-ID ja Smart-ID kuvavad kontrollkoode (et need kuvatakse algul, kuid mitte enam siis, kui ta oma PIN-koodi sisestab), võiks olla kuidagi teisiti lahendatud, et kasutajal oleks võimalik kontrollkoodide vastavust süvenenult kontrollida ka veel PIN-koodi sisestamisel, mitte vaid enne:

Kui on see autentimine [peab silmas Mobiil-ID/Smart-ID kasutamist ja kui rakenduses tuleb ette kontrollkood], siis ju seal ka ikkagi ta [rakenduse kuvatav sõnum] kordab kogu aeg, et loe või jälgi, et see kood oleks sama, mis sulle [sisse logimisel] lubatud./.../ Ma viimasel ajal olen hästi palju tähele pannud seda, et ma unustan seda [kontrollkoodi] sellel hetkel vaadata ja siis on see hetk, kus peab koodi [oma PIN1 või PIN2] sisse panema, aga siis ma enam ei näe seal seda [kontroll]koodi ju. /.../ tegelikult oleks hea, kui samal hetkel [kui sa PIN-koodi sisestad] sul on ka see [kontrollkood] silme ees, sest alguses paned accepti [kinnituse], isegi ei vaata, mis seal kirjas on ja siis on see [kontroll]kood möödas.

22-aastane intervjuueritav

Teenusepakkujate mõjutamine eesmärgiga edendada küberturvalisust

Üks teema, mis samuti intervjuudel tõusetus, on teenusepakkujate mõjutamine. Nii mõned intervjueeritud eksperdid kui ka tavainimesed tõid välja, et küberohtude maandamiseks tuleks senisest süsteemsemalt tähelepanu pöörata teenusepakkujate poolele ja e-keskkondade ohutusele, mitte ainuüksi inimeste käitumise mõjutamisele.

Nii intervjueeritud PPA esindaja kui Pangaliidu esindaja tõdesid, et üht-teist on võimalik teenusepakkujatel teha ka praegu: nt blokeerida kahtlasi veebilehti, piirata neile ligipääsu jms. Samas teenusepakkujate roll olema süsteemsemalt läbimõeldud ja nende vastutus suurem ning seda peaks toetama ka seadusandlus (vt ka ptk 1.2, kus seadusandlusest tulenevaid kitsaskohti mainisime).

Meil on vaja ka neid kanaleid mõjutada [kus petturid tegutsevad] ja iga teenusepakkuja tegelikult peab ise aru saama sellest, kas ja mis roll tal selles on.

Meil on hostingu teenuse pakkujad, kelle kommunikatsioonikanalid, mingid suhtlusäpid, kaughaldustarkvarad... Neid kanaleid tegelikkuses on väga palju, mis tegelikult igaüks natukene võiks rohkem häirida seda protsessi [küberkelmuse toime panemist].

PPA esindaja

Lisaks rõhutasid paar noorema vanuserühma intervjueeritavat, et nende hinnangul peaks seadma rohkem piiranguid suurkorporatsioonidele nagu Google ja Meta, kes oma kasutajate andmeid koguvad. Üks intervjueeritavatest tõdes seejuures, et tema kasutajana tunneb vajadust saada teenusepakkujatele rohkem infot selle kohta, kuidas ikkagi platvormid turvalisust tagavad ja mida nad täpselt selle jaoks ära on teinud:

Millest ma noore inimesena tunnen puudust, on just nimelt agentsus: et ma saaksin ise rohkem teadlikke valikuid teha selle [(oma andmete) küberturvalisuse] kohta. Et teenusepakkujad annavadki mulle aru, mida nad päriselt teevad, et turvalisust tagada.

24-aastane intervjueritav

Infovoldikute jagamine

Mõned just vanema eagrupi esindajad leidsid intervjuudel, et hea viis, kuidas inimestele küberturvalisuse olulisust südamele panna ja neile teadmisi anda, oleks temakohaste infovoldikute jagamine. Seejuures rõhutasid nad, et voldikute sisu peaks kindlasti olema lihtne, selge ja tõstma esile küberturvalise käitumise põhitõdesid koos asjakohaste näidetega. Intervjueritavad, kes infovoldiku jagamise vajadust nimetasid, leidsid, et see võiks inimesteni jõuda posti teel, nagu kunagi saadeti igale leibkonnale ka „Ole valmis!“ trükis¹¹. Üks intervjueritavatest pakkus, et kui vanemaealised inimesed saavad nt telefonioperaatoritelt või teistelt teenusepakkujatele arveid paber kandjal võiks mõnikord ka nt koos arvega sellise infovoldiku kaasa panna.

Ühtlasi arvas üks 58-aastane intervjueritav, et vanemad inimesed hoiaksid kasuliku infoga voldiku tõenäoliselt alles ning saaksid sealt vajaduse korral ikka ja jälle nõuandeid vaadata ehk tegu poleks ühekordselt loetava materjaliga.

Kui mulle tuleks koju mingisugune brošüür, ma võib-olla isegi loeks. Ma arvan, et eakad inimesed loevad kindlasti. /.../ Kui selline asi tuleks koju – sul on see näiteks laua peal. Kui sul tekib probleem, sa saad selle siis sealt üles otsida. /.../ Seda [brošüüri], ma arvan küll, et ikkagi vanemad inimesed kindlasti loeksid. Ma ei tea, kas noored, aga vanemad kindlasti loeksid. /.../ Muidugi, kes ei loe, see ei loe, aga ma arvan, et seda [brošüüri] vist loeks kõige rohkem.

58-aastane intervjueritav

Samal ajal on muidugi ka neid, kes suhtuvad infovoldikute kasulikkusesse skepsisega. Nt tunnistas üks teine 58-aastane intervjueritav, et tema ei usu, et voldikutest oleks kasu, kui vanem inimene ei saa isegi nende sisust aru, ei tunne spetsiifilisi väljendeid jms. Teisalt, võimalik, et infovoldikutest oleks siiski kasu kasvõi meeldetuletava materjalina, nagu mainis ka eelmine tsiteeritav. Samuti võiksid voldikud tõenäoliselt lisandväärtust pakkuda kombinatsioonis personaalse nõustamisega, mida mainisime eespool.

¹¹ „Ole valmis!“ käitumisjuhiste trükis sisaldab tegelikult ühel leheküljel infot ka küberturvalisuse kohta, kuid võib eeldada, et tarbijad ei taju seda materjal spetsiaalselt küberturvalisuse teemale suunatuna ja neil ei pruugi tulla pähe sellest trükisest temakohast infot otsida. Lisaks on teema käsitlemine selles trükises väga napp.

Muud kanalid/formaadid/tegevused

Lisaks eeltoodule kerkis intervjuude käigus esile veel mõningaid viise, kuidas võiks inimeste küberteadlikkust ja -käitumist intervjuueeritavate endi meelest edendada. Järgnev loetelu sisaldab lähenemisi, mida intervjuueeritavad nimetasid pigem üksikutel kordadel, kuid mis on oma unikaalsuses siiski olulised välja tuua:

- Test, mis põhineb individuaalsel sisendil – paar intervjuueeritavat tõdesid, et nad tunnevad puudust lahendusest, kus oleks võimalik ära märkida, milliseid olulisi küberturvalisuse praktikaid nad juba rakendavad ja millistest teemadest rohkem teavad. Seejärel koostaks süsteem vastavalt iga inimese individuaalsele sisendile talle ülevaate sellest, mida too isik peaks veel silmas pidama, et enda küberturvalisuse taset veelgi tõsta. Selline lahendus võimaldaks inimesel üheltpoolt saada hinnang oma valmidusele küberohtusid ära tunda ja vältida ning teisalt annaks ka praktilise sisendi edasisteks tegevusteks.
- Tööriistakast noortele, kes juhendavad eakamaid – üks noorema eagrupi intervjuueeritav leidis, et eakamate inimeste juhendamisel võiks noortele abiks olla tööriistakast. Ta ei täpsustanud ideed pikemalt, kuid eeldatavalt võiks tegu olla abimaterjaliga, mis tooks välja küberturvalisuse põhitõed, mida peaks eakatele edasi andma, kuidas neid selgitada jms.
- Kollektiivsed väljakutsed – mainisime ka peatükis 3.3.2 seoses materiaalsete stiimulitega, et mängustamisel (nt auhinnamängud) võiks olla potentsiaali panna inimesi rohkem küberturvalisuse peale mõtlema. Lisaks klassikalistele preemiatele ja auhinnamängudele, mida seal nimetasime, tõi ka noorema eagrupi intervjuueeritav mängulise lähenemisena välja ka kollektiivseid väljakutseid, milles saaks osaleda koos sõpradega, omavahel võistelda ja seeläbi rohkem inimesi kaasa tõmmata. Heaks näiteks tõi ta seejuures Swedbanki rahatarkuse mängu.
- Küberturvalisusest rääkimine koolide lastevanemate koosolekutel – üks 41-aastane intervjuueeritav nimetas perspektiivika võimalusena, kuidas jõuda rohkemate inimesteni, küberturvalisusest rääkimist lastevanemate koosolekutel. Eeldatavalt võiks teema pakkuda neile huvi eelkõige oma laste turvalisuse tagamiseks, aga ilmselt saaksid paljud lapsevanemad ka ise näpunäiteid ja värskendaksid oma teadmisi.
- Tasulise sisu/tarkvara tasuta kättesaadavaks tegemine õppuritele – tööme peatükis 2.5.2 välja, et sageli lähevad just noored oma küberkäitumises eaturvalisemat teed, sest õpingute käigus on tarvis on ligi pääseda teatud digitaalsele sisule või tarkvarale, kuid puuduvad piisavad ressursid, et ligipääs osta ning seega kasutatakse vajaliku alla laadimiseks kahtlasi veebisaite. Üks 21-aastane intervjuueeritav tõdes, et sellise olukorra vältimiseks ja küberturvalisuse edendamiseks võiks olla vajalikud programmid ja sisu õpingute kontekstis tasuta kättesaadav, et igaüks ei peaks eraldi otsima riskantseid lahendusi materjalide/tarkvara soetamiseks. Kui haridusasutustel ei ole võimalik tasuta ligipääsusid tagada, võiks vähemalt kaaluda märkimisväärsete soodustuste tegemist õppijatele.

3.4.2. Millised sõnumid ja kõneisikud võiksid inimesi kõnetada?

SÕNUMITE SISU

Ole tähelepanelik ja ära usu kõike

Nii noorema kui vanema eagrupi esindajad rõhutasid intervjuudel, et nende hinnangul tuleks küberturvalisuse edendamisel eelkõige üritada inimesteni viia see sõnum, et **tuleb olla tähelepanelik ning kõike ei tasu uskuda**. See põhimõte peaks intervjuueeritavate toodud näidete põhjal kehtima nii digitaalsete materjalide alla laadimisel (pead hoolega silmas, mida sa ikkagi alla laed) kui erineva info tõe pähe võtmisel ja eri üleskutsetega kaasa minemisel.

Oluline oleks küsida [endalt] kindlasti üle mitu korda, millega tegu on. Et ei oleks naiivne.

17-aastane intervjuueeritav

Kõige lihtsam oleks lihtsalt mitte suvalisi asju alla tõmmata. Ei proovi mingit head äppi kuskilt leida, mis tundub nii imeline.

17-aastane intervjuueeritav

See ei ole mitte ainult küberturvalisus, aga üldse kõik sellised teemad, et kui midagi, mida pakutakse, näib liiga hea olevat, et tõsi olla, siis ta ilmselt ka ei ole tõsi. Tasub kahelda algusest peale.

61-aastane intervjuueeritav

Samas tuleks seejuures hoolega mõelda, millises sõnastuses ja millise narratiivi kaudu sellise sisuga sõnumit täpselt edastada, et inimesed võtaksid seda tõsiselt ja saaksid aru, et see põhitõde kehtib kõikide, sh nende puhul. Nt intervjuueeritud küberturvalisuse ekspert tõi välja, et kuna inimesed kipuvad olema usaldavad¹², ei toimi tema hinnangul hästi kampaaniad stiilis „Ära usalda võõrast!“. Eksperdi sõnul ei taju inimesed internetituttavat võõrana, seega ei pruugi selline sõnum nende jaoks kõnekas olla ega pane ka rohkem oma turvalisusele tähelepanu pöörama.

¹² See ilmnes ka meie uuringus, et üks küberhaavatava käitumise ajendeid võib olla kartmatus, mis on tingitud naiivsusest ja liigsest heausklikkusest (vt ptk 2.5.2.).

Sa ei saa öelda kampaanias, et "Ära suhtle võõraga, ära anna talle infot!". See ei ole minu jaoks võõras inimene, kellega ma siin suhtlen oma arust! Sa ei võta seda *awareness'i* [siin kontekstis teadlikkust tõstvat sõnumit] tõsiselt, sest see ei käi sinu kohta. Kui me ütleme seda, et sinu lähedane võib olla petis, on hoopis teine kampaania, kui see, et "Ära suhtle võõraga!". Kui ma juba inimesega suhtlen pool tundi, [siis] ta ei ole võõras. Lapsel on sama asi: "Ära saa võõraga kokku!". Ta ei ole võõras ju – millest sa räägid mulle!? See sõna [„võõras“] – meie arvame, et see on võõras, aga see ei ole talle [inimesele, kellele hoitav sõnum on suunatud] võõras. /.../ Täpselt samamoodi see kampaania peaks olema see, et sinu sõbrad on need, kes sul naha üle kõrvade tõmbavad – sinu internetisõbrad, sinu muud sõbrad, sinu vanemad, sest nad ei oska ja annavad seal [internetis] kõik ära... /.../ Sinu sõbrad on need, kes panevad sinust internetti privaatset infot üles.

küberturvalisuse ekspert

On oluline käia ajaga kaasas, sest kõik on pidevas muutumises

Üks intervjueeritav nimetas olulise sõnumina, mida tuleks inimestele seoses küberturvalisusega südamele panna, seda, et kuna kübermaailmas on kõik pidevas muutumises, tuleb järjepidevalt aja ning arengutega kaasas käia. On tähtis, et inimesed saaksid aru, et nende küberturvalisusalased teadmised ei ole miski, mis saab kunagi „valmis“ – neid teadmisi tuleb ajas revideerida ja värskendada, sest ka ohud muutuvad. Seejuures tõi ta välja tabava paralleeli tervishoiuvaldkonnaga, kus vaktsiinide uuendamist inimestele südamele pannakse:

Küberturvalisusega olekski tegelikult vaja siduda see mantra, mida kõik inimesed teaksidki korrutada: „See teema muutub kogu aeg ja ma pean püsima uudistega kursis selles osas“. /.../ Siin olekski vaja samm ees olla selles osas, et just seda teadvustada, et see [küberturvalisusega seonduv] muutubki kogu aeg. See on fakt ja et see ei ole see, et me õpime ära ja nüüd jääbki kõik staatiliselt niimoodi. /.../ See on ju nagu vaktsiinidegagi – neid on vaja ka uuendada. Sa oled immuunne tolle hetke viiruse versioonile, arvutiviiruste versioonidele või õngitsusajadele, aga see, mis tekib aasta-kahe või kuue kuu pärast, [sellele] sa enam ei ole [immuunne].

24-aastane intervjueeritav

Teisalt tuleb seda sõnumit levitades ka silmas pidada, et on oht tekitada inimestes ärevust ja lootusetut tunnet, et kõik muutubki kogu aeg ja nii palju, et eneses kursis hoidmine on võimatu ning seega polegi mõtet üritada küberturvaliselt käituda. Kirjutasime neist nüanssidest ka peatükkides 2.2.1 ja 2.5.2, tuues välja, et küberturbealase info üleküllus on osale inimestest heidutav.

Telefon ja arvuti – ühed digiseadmed kõik! Või siiski mitte?

Juba varasemates peatükkides (vt ptk-id 2.3.2; 2.5.2 ja 3.2.2) ilmnas, et inimeste küberkäitumises ja ka teadlikkuses võib eri seadmete kasutamise lõikes olla erisusi. Nt töid paar intervjueritavat välja, et nad tajuvad, et nende käitumine on arvutit kasutades turvalisem kui telefoni puhul. Lisaks tõdesid osa intervjueritavatest, et see, mida peaks silmas pidama telefoni turvalisuse puhul, on miski, millest võiks rohkem rääkida.

Niisiis pakkus üks intervjueritavatest välja, et ka küberturvalisusealase info sõnumiseades ja sisulistest (juhend)materjalides võiks rohkem telefoni ja arvutisse puutuvat eristada, et inimesel oleks lihtsam mõista, mida on olulisim just ühe või teise seadme puhul silmas pidada:

Probleem on ka, et need [eri seadmed] kõik on hästi ühes pajas. /.../ Ma tõesti tahaks, et keegi ütleks mulle, et arvutis tee ära need asjad. /.../ Kui keegi ütleks mulle "5 asja, mida ettevõtte arvutis teha!" või "3 asja, mida telefoniga teha!", siis mul oleks ka see, et ma tunnen, et taaskord ma tegin nad [vajalikud tegevused] ära – see on piiratud asi. Ja et keegi ei ütleks mulle, et veel on 10 000 asja, mis ma võiksin teha, et olla kübervaatlik või IT-vaatlik. Mina igatsen lihtsust ja et [küberturvalisusega seotud] teemad [eri seadmete lõikes] oleks lõhestatud.

37-aastane intervjueritav

Rõhuasetus ohtudelt ja kohustuslikelt käitumispraktikatelt üldisemale hüvele ning sellele, kui atraktiivne on olla küberturvaline

Paar intervjueritavat nooremast ja keskmisest vanuserühmast leidsid, et kuna küberturvalisus ei ole üldjuhul teema, mis inimestele väga huvi pakuks ja tegutsemisindu tekitaks, tuleks küberturvalisusealastes sõnumites fookus viia ohtudelt ja rangetelt soovituselt või kohustuselt turvaliselt käituda hoopis sellele, mis on küberturvalise käitumisega kaasnevad positiivsed aspektid. Nt üks intervjueritavatest tõi välja, et kui küberturvalisusega ei seostuks tema jaoks asjad, mida tuleb teha, vaid pigem suurem pilt sellest, mille hüvanguks küberturvaline käitumine vajalik on, oleks tal rohkem motivatsiooni teemaga tegeleda:

Ma ise tegelikult teen ka selle vea või selle teevad ka teised, et küberturvalisus tundub mulle selline korrastamise ja... Tüütu teema – ma ütlen otse. Mitte sellepärast, et ta on vale, vaid ta lihtsalt tundub mulle tüütu. Võib-olla ta vajab ümbervormistamist. Näiteks kui me ütleks, et [küberturvaline käitumine] on patriootlik või et on baasturvalisus – et ta puudutaks minus mingeid hingekeeli natuke rohkem – võib-olla siis ma võtaks selleks aja [küberturvalisust rohkem silmas pidada].

37-aastane intervjueritav

Teine, noorema eagrupi esindajast intervjueritav pakkus aga välja, et selmet rääkida riskistsenaariumitest, mida paljud inimesed tõsiselt ei võta, sest nad ei usu iseenda ohvriks langemist (käsitlesime seda uskumust pikemalt ptk-s 2.5.2), võiks küberturvalisusalase info keskmesse seada hoopis selle, kui atraktiivne on olla küberteadlik inimene, kes elab küberturvalist elu:

/.../ mis praegu on natukene reha, mille otsa on astunud, on see, et kui me räägime küberturvalisusest, siis me räägime hästi palju selle stsenaariumi läbi, mis võib juhtuda. Ja seal on alati see oht, et ma tunnen: “Aga mis see tõenäosus on, et see minuga juhtub?”. Ma olen alati valmis võtma seda riski, et “Mina olen kindlasti see 1%, kellega see kunagi ei juhtu”. Aga võib-olla tuleks narratiiv pöörata ümber. Ehk me peaksime seda lugu jutustama sellega, mis kindlasti juhtub, kui sa oled küberteadlik. Ja kui me nüüd suudaksime kasvõi riigi sees luua küberteadlikust ja küberturvalisest inimesest kuvandi kui väga atraktiivsest inimest, et /.../ seksikas on olla küberturvaline, siis tegelikult see on see, mida sa saad. Iga tegevus, mida ma teen, et ma oleksin rohkem küberturvaline, muudab mind ja minu enda peegelpilti minu silmis kuidagi atraktiivsemaks. Ja see on see 100% kindlus, mis kindlasti juhtub.

24-aastane intervjueritav

KÕNEISIKUD

Keegi, kellega inimene samastub või kes tundub lahe eeskuju: noortele suunamudijad, eakatele Alma „Õnne 13st“, ettevõtjatele teised ettevõtjad

Nii intervjueritud noored kui ka üks keskmise vanuserühma esindaja tõdesid, et kui viia ellu noortele suunatud küberturvalisusalaseid ennetus- ja teavitustegevusi, võiks noortes huvi äratamiseks kaasata kampaniasse/tegevustesse suunamudijaid või kuulsusi, kes noori kõnetavad. Noorema vanuserühma intervjueritavad meenutasid seejuures ka mitmeid teisi valdkondi, kus sellist taktikat on kasutatud: Tervise Arengu Instituut kaasab taldrikureegli õpetamisse Maria Rannavälja; täiskasvanuhariduse ja haridustee jätkamise populariseerimisel kasutati Tanel Padari kogemuse jagamist; noored suunamudijad on kajastanud sotsiaalmeedias rahatarkuse teemat.

Üks intervjueritud noortest tõdes, et seejuures võiks ka kaaluda, kuidas hariva ja meelelahutusliku sisu saaks ühendada, et noortes teema vastu huvi tekitada:

See ei peagi olema alati hariv sisu. Kui näiteks [sotsiaalmeedias jagatavate] lühivideote peale mõelda: see võib ka olla meelelahutuslik pool, aga sinna sisse on lükatud mingeid harivaid noote.

24-aastane intervjueritav

Ühtlasi pakkusid intervjuueeritavad välja, millistel viisidel saaks küberturvalisuse teemal suunamudijate potentsiaali ära kasutada: nt saaksid suunamudijad rääkida enda kogemustest seoses küberohtudega ja tuua õpetlikke näiteid või koguda oma jälgijaskonnalt hoiatavaid lugusid sellest, mis on juhtunud, kui küberturvalisuse põhitõdesid pole järgitud.

Mina ise Eesti *influencereid* [suunamudijaid] üldiselt ei jälgi, aga ma tean, et suurem osa minu eakaaslasi jälgivad neid, seega ma arvan, et nende [küberturvalisusteemalised] jutud töötaksid. Nad võiksid küsida oma fännidelt, et saatke mulle jutte [oma kogemustest], ma saan neid anonümselt rääkida. Ja siis lihtsalt jagadagi teiste kogemusi. Et *influencer* soovib ise rohkem teada sellest [küberturvalisusest] ja siis ta saab jagada ka seda teadmist.

17-aastane intervjuueeritav

Kui kasvõi näiteks Eesti omadega [peab silmas suunamudijaid] midagi koostöös teha, kus nad räägiksidki /.../ nende enda kogemustest. /.../ Mis juhtub, kui Youtuberid... et nende kanaleid häkitakse. Võib-olla näiteks selle nurga alt, et rääkidagi, et inimese elutöö oleks peaaegu ära kadunud. Et see asi võib juhtuda sinuga, sa ei pea olema suur Youtuber selleks – su konto võidakse Facebookis kasvõi ära varastada lihtsalt selleks, et saata õngitsuslinke su sõpradele.

24-aastane intervjuueeritav

Samastumisega seoses tõstsid mitmed intervjuueeritavad esile ka seda, et **tavainimese käitumist võib aidata mõjutada see, kui ta näeb, kuidas toimivad temasarnased inimesed nt teleseriaalides**. Eeskätt vanematest inimestest ja nende küberkäitumise mõjutamisest rääkides, tõusetus nii ekspertide kui noorema vanuserühma intervjuudel mõnel korral mõte sellest, et (vanemad) inimesed saaksid õppida nt teleseriaali „Õnne 13“ tegelaste käitumismustritest ja sellest, kuidas seal üleskerkinud probleeme on lahendatud.

„Õnne 13“, kõik erinevad seriaalid – kui seal midagi on [küberturvalisuse teemadel] sees ja seal midagi juhtus, mida inimesed [seriaali tegelaskujud] lahendasid, siis need käitumismustrid võetakse [tavainimeste poolt] kasutusse.

küberturvalisuse ekspert

Olgugi et selle uuringu fookuses on eelkõige tavakasutajate käitumise mõjutamine püsivalt küberturvalisemaks, piltlikustab seda, et samastumise aspekt on kõneisikute valimisel äärmiselt oluline, ka intervjuueeritud ITL-i esindaja tõdemus selle kohta, et nende kogemuse järgi on **ettevõtjate küberkäitumise mõjutamiseks tarvis sõnumi levitajaks teist ettevõtjat**.

Info noorelt eakale

Intervjuude käigus tuli nii mõnelgi korral jutuks, et eakamate inimesteni jõudmisel võiks abiks olla noored. Nt avaldas intervjuueeritud Pangaliidu esindaja lootust, et nooremad inimesed võiksid olla need, kes harivad küberturvalisuse teemal ka oma vanemaid ja

vanavanemaid. Samuti töid mõned keskmise eagrupi intervjueeritavad välja, et nooremad pereliikmed võiksid olla oma eakamate sugulaste jaoks küberturvalisusalase info vahendajad ja need, kes aitavad paika panna digiseadmete turvasätteid jms. Üks intervjueeritud noortest rõhutas ühtlasi, et oluline ongi tõsta just noorte teadlikkust, et nemad saaksid olla kanal, mille kaudu vanemaid inimesi küberturvalisuse alal haritakse ja/või toetatakse:

Kui noored inimesed saavad aru sellest, et see [küberturvalisusele tähelepanu pööramine] on vajalik, siis nad oskavad paremini toetada internetis ka enda vanemaid, enda vanavanemaid. See on hästi oluline, et ma ise oleks [küberturvalisusega seonduvaga] kursis ja saaksin neile [oma (vana)vanematele] siis seletada, miks mingi asi oluline on. Võib-olla vanemate inimeste puhul [on] ka see generatsiooniline vahe, et nad kohati usuvad kõike ja samas ei usu mitte midagi. Aga kui [küberturvalisusalane] info tuleb nende enda nooremalt sugulastelt, siis võib-olla võetakse asja natuke tõsisemalt.

23-aastane intervjueeritav

Tõime ka peatükis 3.1, kus andsime ülevaate sellest, kust saavad inimesed küberturvalisusalast infot, välja, et vanemad inimesed küsivad kahtluse või oskamatus korral sageli nõu nooremate sugulaste (eeskätt oma laste) käest. Seega võib öelda, et info vahendamine noortelt eakamatele toimub ka juba praegu, kuid lähenemine saaks olla süsteemsem ja laialdasemalt levinud. Näide, kuidas üksikutes kohtades sellist noorelt vanemale nõustamist rakendatakse, tuli välja ka ühel vanema eagrupi esindajaga läbiviidud intervjuul, kus intervjueeritav tõstis esile, et nende kohalikus raamatukogus toimuvad „Muna õpetab kana“-koolitused, kus noortekeskuse noored aitavad vanemaealistel jagu saada konkreetsetest probleemidest, mis on tekkinud kas nutitelefonis, sülearvutis või laiemalt internetis toimetades.

Vahekokkuvõte

Eesti inimesed saavad küberturvalisuse kohta informatsiooni erinevatest allikatest: massi- ja sotsiaalmeediast, teistelt inimestelt (nt pere- või sõpraderingis) ning ka töökoha või (kõrg)kooli kaudu.

Üldiselt on inimesed seisukohal, et küberturvalisusalast informatsiooni leidub piisavalt, ent samas tõdetakse, et asjakohane info ei pruugi alati ette sattuda ja huvi või mure korral tuleb sel juhul vajalikku teavet ise otsida. See, kui palju tuleks küberturvalisusalast infot avalikkuses ikka ja jälle üle korrata, tekitab Eesti elanikes vastakaid tundeid: osa inimeste hinnangul on teema pidev üle kordamine kasulik ja aitab küberturvalisuse olulisust meeles hoida, kuid leidub ka neid, kelle meelest on küberturvalisusalast infot liiga palju ja see hakkab seetõttu muutuma tüütavaks, mis

omakorda võib viia selleni, et inimesed lülitavad end teemakohasest infovoost välja.

Küberturvalisusega seotud teemad, mille kohta inimesed rohkem teavet soovivad, on eelkõige tehisaru ja selle kasutamisega seonduv, (isiku)andmete kaitsmine ja privaatsus ning ka turvaliste paroolide rakendamine. Eri sihtrühmade infovajadus võib seejuures olla erinev – kui nt noored sooviksid saada rohkem süvitsiminevat, nii-öelda edasijõudnute taseme informatsiooni, siis vanemate vanusegruppide seas on tulenevalt info üleküllusest vajadus selge ja lihtsal moel esitatud teabe järele, mis kordab üle küberturvalisuse põhitõdesid.

Pelgalt üldised küberturvalisusalased hoiatused või kuiv informeerimine ei pruugi inimeste küberkäitumist mõjutada. Küberturvalisusele suurema tähelepanu pööramisel on mõjus motivaator reaalelulised juhtumid ehk isiklik kogemus küberintsidendiga või kellegi teise (sh lähedase) kogemuslugu. Päriselu näited aitavad inimestel teadvustada, et ohud pole kauged ega teoreetilised, vaid võivad tabada igäüht, sõltumata inimese taustast. Eriti hästi mõjuvad lood, millega on lihtne samastuda – need peavad olema ajakohased ja rääkima inimestest, kes sarnanevad kuulajaga. Simuleeritud kogemused, nt kübertestid, -õppused või mängulised stsenaariumid võivad samuti pakkuda ohutut viisi riskide mõtestamiseks. Ühtlasi võivad motivaatorid olla välised: nt rahalised preemiad ja auhinnad nagu kinkekaart või allahindlus, mis suunavad inimest küberturvalisemalt tegutsema. Samas on sellisel materiaalsetel stiimulitel põhineval lähenemisel ka piirangud – preemiate ajendil käitumine võib jääda formaalseks või tekitada inimestes skepsist.

Inimeste küberteadlikkuse ja -käitumise edendamiseks on tarvis kasutada tõhusaid ja sihtrühmadele vastuvõetavaid käitumise mõjutamise viise. Kanalitest, formaatidest ja tegevustest, mida Eestis küberturvalisuse edendamisel juba rakendatakse või on rakendatud, tasub ka edaspidi kasutada massi- ning sotsiaalmeedias info jagamist ning ka praktiliste, osalejaid kaasavate koolituste korraldamist. Samuti on inimeste küberturvalisusalane harimine koostöös tööandjatega mõjus ja nutikas viis, mida võiks rakendada senisest laialdasemalt.

Uutest või senisest olulisemalt süsteemset rakendamist eeldavatest kanalitest, formaatidest ja tegevustest vajaksid Eesti elanikud enda hinnangul eelkõige küberturvalisusalast personaalset nõustamist nt infoliini või veebipõhise platvormi kaudu (eriti nooremate inimeste puhul) ja ka individuaalse konsultatsiooni või väikeste töötubade/õpiringide formaadis (vanemate inimeste puhul). Kombinatsioonis personaalse nõustamisega võiksid (eeskätt eakamatele inimestele) lisaväärtust pakkuda ka lihtsa ja selge sisuga infovoldikud, mis tuletaksid inimestele meelde küberturvalise käitumise põhitõdesid koos asjakohaste näidetega.

Muuhulgas on Eesti elanike hinnangul oluline lõimida küberturvalisuse edendamine süsteemsemalt haridusasutuste tegevustesse nii läbi sisukama teemakäsitluse

ainetundides kui ka nt (kõrg)koolides korraldatavate küberõppuste ja -testide kaudu. Ühtlasi on küberturvalisuse edendamisel tarvis rohkem tähelepanu pöörata võimalustele võtta kasutusse enam toetavaid tehnoloogilisi lahendusi ja meeldetuletusi. Tähtis on ka koostöö teenusepakkujatega, et tagada e-keskkondade ohutus. Peale eeltoodu võib inimeste sõnul küberturvalisuse edendamisel potentsiaali olla ka vastavasisuliste kollektiivsete väljakutsete korraldamisel; testil, mis annab inimesele individuaalsel sisendil põhineva ülevaate küberturvalisuse tagamiseks vajalikest sammudest; tööriistakastil, mida noored saaksid kasutada eakate juhendamisel; koolides lastevanemate koosolekutel küberturvalisusest rääkimisel ning ka tasulise sisu/tarkvara tasuta kättesaadavaks tegemisel õppuritele, et nad ei läheks vajalike materjalide otsimisel ebaturvalisemat teed.

Eesti elanikud leiavad, et küberturvalisuse edendamisel on eelkõige oluline inimestele südamele panna, et internetis toimetades tuleb olla tähelepanelik, kõike ei tasu uskuda ning oluline on käia ajaga kaasas ja värskendada alatasa oma küberturvalisusalaseid teadmisi, kuna kõik on pidevas muutumises. Ühtlasi võiks küberturvalisusealase info levitamisel katsetada lähenemist, kus fookus on viidud ohtudelt ja rangetelt soovitustelt või kohustuselt turvaliselt käituda hoopis üldisemale hüvele ning sellele, kui atraktiivne on olla küberturvaline.

Küberturvalisuse alase info jagamisel ja selle jõudmisel sihtrühmadeni peavad inimesed tähtsaks kõneisikute rolli, kes võiksid eelkõige olla isikud, kellega sihtrühmade esindajad samastuvad ja/või kes on sihtrühma jaoks autoriteetsed (nt noorte puhul suunamudijad ja/või kuulsused, ettevõtjate puhul teised ettevõtjad jne). Eakamate inimesteni jõudmisel võiks aga abiks olla noored, kes võiksid vähemalt oma vanemate sugulaste jaoks olla kanal, mille kaudu eakaid küberturvalisuse alal haritakse ja toetatakse.

4. (Küber)käitumist püsivalt mõjutavad sekkumised ja nende rakendatavus Eestis

Lisaks sellele, et selle uuringu eesmärk on aidata RIA-l paremini mõista Eesti elanike küberturvalist käitumist, millele keskendusime eelnevates peatükkides, on ühtlasi uuringu siht selgitada välja võimalikud sekkumised¹³, mis tulemuslikult aitavad mõjutada inimeste käitumist püsivalt küberturvalisemaks. Samuti on eesmärk hinnata nende sekkumiste rakendatavust Eesti kontekstis.

Mitmed tuntud teooriaid käsitlevad inimeste käitumise muutmist: nt planeeritud käitumise teooria (Ajzen, 1991), transteoreetiline mudel (TTM; Prochaska & Velicer, 1997) ning Rogersi (1983) kaitsemotivatsiooni teooria, mis paljude uurijate hinnangul (nt Alsharida *et al.*, 2023; Haag *et al.*, 2021; Kiran *et al.*, 2025; Siponen *et al.*, 2024) sobitub enim ka just küberturvalise käitumise valdkonda. Siiski ei suuda käitumise muutmise teooriad sageli inimeste tegelikku käitumist selgitada või ei õnnestu nende abil alati käitumist muuta. Peamiselt seepärast, et inimesed ei käitu alati ootuspäraselt või „ratsionaalselt“. Seejuures on küberturvalist käitumist edendavate kampaaniate ebaõnnestumise põhjustena varem välja toodud nt sihtrühmale liiga üldise ja ebapraktilise teabe edastamist ning tagasisidestamise puudumist (Bada *et al.*, 2019).

Varasemates küberkäitumise edendamist käsitlevates uuringutes on nt rõhutatud, et organisatsioonide kontekstis on töötajate küberturvalise käitumise parandamiseks tarvis teadmiste kõrval uurida ja adresseerida ka töötajate hoiakuid: riskitaju ja riskantse küberkäitumise tajutud eeliseid ja kasu (Glaspie *et al.*, 2018; Pollini *et al.*, 2022). See on oluline, sest tähtis on just töötajate suhtumine küberturvalisusega seotud reeglitesse, mitte ainuüksi asjakohaste teadmiste olemasolu. Lisaks on Chaudhary (2024) järgi küberturvalise käitumise – eelkõige organisatsiooni kontekstis – parandamiseks oluline asutuse juhtkonna osalemine küberturvalisusalastes tegevustes, küberturvalisuse edendamine kui järjepidev ja uuenev protsess, küberturvalise käitumise soosimine preemiatega ja positiivse tagasisidega, efektiivsete ja selgete küberturvalisuse sõnumite kujundamine ning küberturvaline käitumine kui ühine norm ja oluline osa inimeste identiteedist.

Viru (2025) on Eesti vanemate täiskasvanute küberturvalisele käitumisele keskendunud magistritöös samuti rõhutanud isikliku tähenduse olulisust küberturvalise käitumise püsival muutmisel. Küberturvalise käitumise püsivaks muutmiseks vajaliku sekkumise komponentidena tõi ta eksperdiintervjuude ja Kwasnicka *et al.* (2016) põhjal välja soovitud käitumise korduva kinnistamise ja igapäevaellu toomise ning sekkumise järjepidevuse.

¹³ Tuletame meelde, et sekkumise all peame silmas sihipärast tegevust, strateegiat või meetet, mis on suunatud üksikisikutele või rühmadele ning mille eesmärk on muuta (küber)käitumist, parandades inimeste teadlikkust, hoiakuid või harjumusi.

Eelnevast selgub, et **varasemad uuringud on küll käsitlenud nii küberturvalist käitumist mõjutavaid isiklikke ja organisatsioonitasandi tegureid ning küberturvalist käitumist edendavaid sekkumisi, ent siiski pole teadlaste seas konsensust selle osas, mis on inimeste küberkäitumise püsivaks parandamiseks kõige parem viis (Almansoori *et al.*, 2023).** Seetõttu on oluline analüüsida erinevate käitumise muutmise tehnikate mõju empiiriliste andmete põhjal. **Meile teadaolevalt pole varem süstemaatiliselt pikaajaliselt ja püsivalt just küberkäitumist mõjutavaid sekkumisi uuritud.** Siin ja edaspidi peame püsiva mõju all silmas vähemalt kuus kuud pärast sekkumise rakendamist tuvastatavat positiivset muutust.

Selleks, et koondada kokku parimad tõendus põhised sekkumised, mis inimeste käitumise, sealhulgas küberkäitumise püsivaks mõjutamiseks eksisteerivad, teostasime uuringu esimeses etapis **süstemaatilise kirjandusülevaate** (vt kirjandusülevaate metoodika kohta täpsemalt Lisa 1. Meetodid ja andmed). Vastavalt uuringu tellija koostatud lähteülesandele **käsitlesime ülevaates korraga nii üldisemaid käitumise mõjutamise mehhanisme ja sekkumisi, millel on tuvastatud püsiv mõju, kuid otsisime ka spetsiifiliselt küberkäitumise mõjutamisele keskendunud sekkumisi.**

Kaasasime ülevaatesse järgmistele kriteeriumitele vastavad uuringud:

- käsitletakse sekkumisi käitumise või hoiakute muutmiseks;
- uuringu osalejad on vähemalt 16-aastased inimesed;
- mõõdetakse tulemustena käitumise püsiva muutusega (vähemalt kuus kuud) seotud tunnuseid;
- tegemist on metaanalüüsi või süstemaatilise ülevaateuuringuga;
- avaldatud viimase viie aasta jooksul.

Kõik seatud kriteeriumite järgi ülevaatesse kaasatud sekkumised või mehhanismid kategoriseerisime nende käitumise muutmise tehnikate järgi (Michie *et al.* 2019 *behaviour change techniques taxonomy (v1)*), et uuringu järgmistes etappides oleks võimalik ülevaatest esile kerkinud mõjusaid tehnikaid sobitada just uuringusse hõlmatud eri vanuses Eesti elanike turvalist küberkäitumist motiveerivate tegurite, küberhügieeni võimekuse ning võimalustega.

Sekkumisi, mis süstemaatilise kirjandusülevaate teostamise järel sõelale jäid, kirjeldasime järgmiste näitaja abil: sihtrühm, valdkond, sekkumise sisu, käitumise muutus, peamine käitumise muutmise tehnika, püsiva mõju tõendus ning hinnang rakendatavusele.

Kõik sekkumised, mida kirjeldasime ning mille rakendatavust hindasime, on koondatult esitatud järgnevalt toodud tabelis (vt Tabel 1).

Tabel 1. Süstemaatilise kirjandusülevaate tulemused: käitumise mõjutamise sekkumised ja nende rakendatavus

Sekkumine	Sihtrühm	Valdkond	Sekkumise sisu	Käitumise muutus	Käitumise muutmise tehnika(d)	Püsiv mõju
Tagasisidestatud kaugmonitoorimine Peiris <i>et al.</i> (2023)	Metaboolse sündroomiga täiskasvanud	Tervis	Terviseinfo sessioon, millele järgneb kaugmonitoorimine regulaarse tagasisidega (e-kiri või telefonikõned)	Kehalise aktiivsuse harjutuste tegemine või ettekirjutuste järgimine (objektiivsed mõõdikud, nt sammulugeja statistika või eneseraporteerimine päevikuvormis)	Tagasiside ja monitoorimine	Jah

Rakendatavus: madal

Sekkumine oleks küberturvalisuse valdkonnas rakendatav vaid RIA ja pankade või telekommunikatsiooniettevõtete koostöös ning juhul, kui valitakse väga kitsas sihtrühm – muul juhul liiga kulukas. Lisaks saab küberhügieeni distantsilt monitoorida vaid teenusepakkuja, mis muudaks sekkumise rakendamise veelgi keerukamaks. Ühtlasi on küsitav, kuidas oleks võimalik kaugmonitoorimise ajal tagada inimeste privaatsus internetis toimetamisel.

Sekkumise rakendamine eeldab sihtrühmalt järjepidevust ja motivatsiooni tegevuses osaleda, mida ei pruugi inimestel küberturvalisuse valdkonnas eriti olla, kuna tervisevaldkonnas võib saadav kasu olla inimesele endale kergemini tajutav kui küberturvalisuse puhul.

Individuaalselt kohandatud motiveeriv suuhügieeni-programm (ITOHEP) Abbinante <i>et al.</i> (2024)	Täiskasvanud	Tervis	Individuaalselt kohandatud motiveeriv suuhügieenialane programm, mis põhineb kognitiiv-käitumuslikel põhimõtetel ja motiveerival intervjuerimisel. Motivatsioonisõnumite pidev kordamine viib pikaajalise muutuseni.	Pikaajaline suuhügieeni järgimine igemeravis	Teadmiste kujundamine, eesmärkide seadmine, planeerimine ja enese-monitoorimine	Jah
--	--------------	--------	--	--	---	-----

Rakendatavus: kõrge

Kogu elanikkond oleks selle sekkumise rakendamiseks küberturvalisuse valdkonnas liiga mahukas sihtrühm. Kübervaldkonnas oleks võimalik sekkumist rakendada nt koostöös tööandjatega, pakkudes programmi töökohal. See võimaldaks ka individualiseerida – nt läheneda organisatsiooni sees vastavalt sellele, kas inimene töötab arvutiga; milliseid elektroonilisi teenuseid tööks kasutab; milline on töö iseloom jne. Programmi töökohapõhine rakendamine aitaks ühtlasi tagada korduvuse kui sekkumise olulise elemendi säilitamist. Sekkumise rakendamise eeldus on, et tööandjatel oleks huvi programmi rakendada. Tööandjate motivatsioon osaleda on tõenäoliselt suurem siis, kui programmi rakendamine on ettevõtte jaoks tasuta, mis tähendab, et sekkumise elluviimisest huvitatu peab tagama ka vajalikud ressursid. Peale koostöö ettevõtetega võiksid võimalikud partnerid sekkumise rakendamisel kitsamas sihtrühmas olla ka nt Väärivate Ülikoolid, vabaühendused või organisatsioonid, kes tegelevad nt uussisserändajate kohanemise toetamisega.

Programmi küberturvalisuse konteksti kohandamisel võiks sekkumine koosneda järgnevatest komponentidest:

1. [Teadmiste taseme, ootuste ja motivatsiooni analüüs](#). Kõigepealt hinnatakse, mida inimene juba küberhügieeni kohta teab, millised on ta ootused (nt soov tunda end turvaliselt internetis ostlemisel) ning peamine motivatsioon, nt rahalise kahju vältimine.
2. [Inimese seniste küberturvalisuse praktikate analüüs](#), kus tuvastatakse nii head harjumused kui ka riskantsed käitumismustrid.
3. [Küberturvaliste oskuste harjutamine](#) eesmärgiga tagada, et inimene tunneks end vajalikke tööriistu (nt paroolhaldurid, privaatsusseadete muutmise) kasutades enesekindlalt, mitte ei mõistaks neid vaid teoorias.
4. [Individaalsete küberkäitumise eesmärkide seadmine](#). Eesmärgid peavad vastama inimese võimekusele ja olema ta igapäevast digielu silmas pidades asjakohased.
5. [Järjepidev enesemonitoorimine](#), oskuste või teadmiste kontroll nt testi vm mängustatud vormis.
6. [Küberturvalise käitumise üldistamine](#) ehk heade praktikate ülekandmine erinevatesse kontekstidesse. Kui kasutatakse tugevaid paroole tööl, siis tehakse seda tõenäolisemalt ka isiklikel kontodel ning kui tuntakse andmepüügi ohte e-posti kasutades, siis saab samu oskusi rakendada ka sõnumirakendustes.
7. [Soovitud küberkäitumise säilitamine](#). Tuleb toetada pikaajaliste harjumuste kujundamist, kasutades nt meeldetuletusi turvauuenduste kontrollimiseks, ning planeerida, kuidas käituda n-ö tagasilanguse korral.

<p>Mitme teooria mudelil (<i>multi-theory model</i>, MTM) põhinevad sekkumised tervisekäitumise muutmiseks</p> <p>Kapukotuwa <i>et al.</i> (2024)</p>	Üldine, erinevad	Tervis	<p>Mitme teooria mudeli sekkumised toetavad kahte käitumise muutmiseks vajalikku komponenti: muutuse algatamist ja säilitamist. Algatamisel keskendutakse kaasavale dialoogile, enesekindluse tõstmisele ja muutustele füüsilises keskkonnas, arutletakse käitumise muutmise plusside ja miinuste üle koos professionaaliga. Muutuse säilitamise faasis on fookuses käitumise harjutamine ja muutust toetava sotsiaalse keskkonna loomine.</p>	Erinevad: HPV vaktsineerimine, vesipiibu suitsetamise vähendamine, tervislik toitumine, füüsiline aktiivsus	Plussid ja miinused, teave tervisemõjude kohta, endasse uskumine, negatiivsete emotsioonide vähendamine, käitumise harjutamine, sotsiaalne tugi	Jah
--	------------------	--------	--	---	---	-----

Rakendatavus: keskmise

Sekkumine oleks küberturvalisuse valdkonnas rakendatav eeldusel, et eksisteerib sihtrühm, millel oleks mingisugune ühisosa ja kelle käitumise muutus sihiks seatakse (nt ettevõtjad). Ettevõtete juhid võiks tõenäoliselt olla motiveeritud osalema, kui sekkumise rakendamise tulenev käitumise muutus aitaks kuidagi vähendada äririske. Ekspertid pidasid sekkumise erinevaid elemente rakendatavateks, kuid tõenduspoolel eksisteerib just mitmest komponendist koosneva sekkumise kohta ja pole selge, kui tõhusad oleksid üksikud elemendid.

<p>Preemiad prügi sorteerimise eest</p> <p>Trushna <i>et al.</i> (2024)</p>	Üldine, erinevad	Tarbimine, keskkond	<p>Preemiatena raha, sooduskupongid või boonuspunktid ning ka mitterahalised preemiaid nagu kompostikotid ja loosiauhinnad.</p>	Erinevad kodumaja-pidamises prügi sorteerimisega seotud muutujad: sorteeritud jäätmete kaal, sorteerimisega seotud	Preemiad ja ohud	Jah
--	------------------	---------------------	---	--	------------------	-----

					hoiakud, jäätmete hulk vales konteineris
--	--	--	--	--	--

Rakendatavus: keskmine

Sekkumise küberturvalisuse valdkonda kohandamiseks vaja välja valida konkreetsed sihitavad käitumised – nt paroolide vahetamine, tarkvara uuendamine. Sekkumise pluss on, et võimalik on sihtida korraga suhteliselt laia sihtrühma. Samas kitsaskoht on selle sekkumise puhul see, et rahaliste preemiade pakkumine pole RIA kui riigiameti jaoks sobilik/kohane.

Küberturvalisuse valvurid vanemaealistes kogukondades	Vanemaealised	Küberturvalisus	Üheksa kuud kestev kogukonnapõhine küberturvalisuse algatus, mille eesmärk on toetada vanemaealisi küberturvalisusalaste teadmiste omandamisel (koolitatud "CyberGuardians") ja parimate praktikate jagamisel eakaaslastega	Küberturvalisuse teadlikkuse ja küberkäitumise paranemine, küberkäitumise teemaliste vestluste normaliseerimine kogukonnas	Teadmiste kujundamine (<i>peer-to-peer</i>)	Ei mõõdetud
Nicholson <i>et al.</i> , (2021)						

Rakendatavus: keskmine

Sekkumist saab soovi korral kohandada lisaks vanemaealistele ka teistele sihtrühmadele. Küberturvalisuse „valvuri“ rolli võivad kanda ka nt raamatukogude töötajad, kuid tuleb arvestada, et nad on oma praeguses rollis juba niigi ülekoormatud. Kaaluda võiks, kas ja milline võiks olla naabrivalve roll kogukonnapõhises küberturvalisuse edendamises.

Neljakordne „E“ lähenemisviisi tõhusa küberhügieeni tagamiseks	Üliõpilased	Küberturvalisus	Integreeritud küberhügieeni mudel käitumise parandamiseks, mis hõlmab nelja etappi: harimine (<i>educate</i>), avastamine (<i>explore</i>), teostamine (<i>execute</i>) ja hindamine (<i>evaluate</i>)	Küberhügieenialane teadlikkus ja käitumine	Teadmiste kujundamine	Ei mõõdetud
Salem ja Sobaih (2023)						

Rakendatavus: kõrge

Kuigi üliõpilased pole seni eraldi RIA ennetus- ja teavitustegevuste sihtrühmade hulka kuulunud, oleks sekkumine teiste väljatoodud sekkumistega võrreldes kergesti ülevõetav ning võiks sisuliselt toimida, kui RIA olemasolevaid tegevusi lihtsalt kõrgkoolidele kui omaette sihtrühmale laiendada. Sekkumise neli etappi hõlmavad loenguid ja õppematerjalide jagamist küberturvalisuse teemal, iseseisvat õppimist ja enesetestimist, õpitu rakendamist oma seadmetes/kontodel ning viimaks tulemuste hindamist. Sekkumise rakendamine eeldab RIA koostööd kõrgkoolidega, kellega tuleks kokku leppida õppevorm ning panna ühiselt paika õppemoodulite ja õppematerjalide sisu, pidades seejuures silmas nende korduvkasutatavust ja uuendamist vastavalt muutuvatele küberohtudele. Üliõpilasi võiks osalema motiveerida sekkumise integreerimine mõne kohustusliku või valikõppeainega. Õppemoodulid peaksid käsitlema nii teoreetilist tausta (nt küberhügieeni definitsioon, kasutegurid jms) kui ka praktilisi küberhügieeni nõuandeid (nt paroolide turvalisus, mobiiltelefoni turvalisus jne). Iseseisvat õppimist ning enesetestimist saab toetada Moodle'i või muude e-õppe platvormide kaudu, mis võimaldavad üliõpilastel oma teadmisi kinnistada interaktiivsete ülesannete ja testide abil. Selleks, et toetada õpitu rakendamist

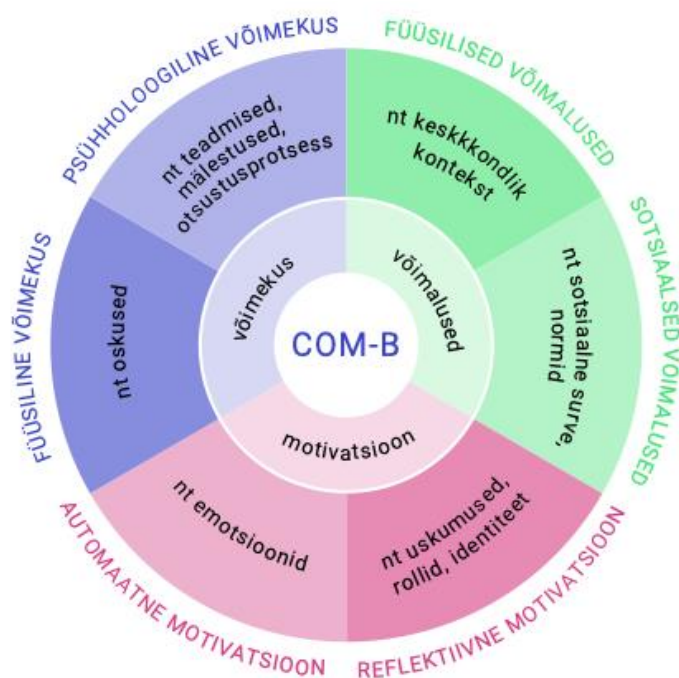
oma seadmetes/kontodel saab õpilaste jaoks välja töötada nt vajalike tegevuste kontrollnimekirja, et nad saaksid üle vaadata, kas ja mida peaks veel silmas pidama, et enda küberhügieeni parandada.

5. Eesti elanike küberturvalise käitumise toetamiseks sobivate sekkumiste ja lünkade kaardistus

Selles peatükis sünteesime süstemaatilise kirjandusülevaate ja intervjuude analüüsi tulemused, eesmärgiga tuvastada Eesti elanike küberturvalise käitumise toetamiseks sobivad sekkumised. Lisaks on siinse kaardistuse eesmärk tuvastada võimalikke lünki küberturvalist käitumist edendavate sekkumiste pakkumises Eestis, võttes arvesse Eesti elanikele iseloomulikke käitumismustreid, mis uuringu käigus selgusid.

Peamiste tööriistadena kasutame käitumismuutuste ratast (ingl *the Behaviour Change Wheel - BCW*) ja sellega seotud COM-B mudelit (Michie, 2011), mis aitavad mõista inimeste käitumise taga olevat võimekust, võimalusi ja motivatsiooni ning kujundada neid komponente sihtivaid sekkumisi. COM-B/BCW mudel on erinevates valdkondades käitumise muutmise sekkumiste disainimisel laialt kasutusel (Alshaikh *et al.*, 2019; Hedin *et al.*, 2019; Kolodko *et al.*, 2021) ning see sobib ka küberturvalise käitumise analüüsimiseks ja edendamiseks hästi, sest pakub mitmekülgset, kuid samas praktilist raamistikku inimkäitumise mõjutajate mõistmiseks. COM-B/BCW mudel ei käsitle inimesi kui alati ratsionaalselt käituvaid olendeid, vaid võtab selgelt arvesse inimeste võimekuse, võimalused ja motivatsiooni kui koostoimelised tegurid, mis käitumist kujundavad. Lisaks on COM-B/BCW mudel käesolevas uuringus asjakohane, sest see seob võimekuse, võimalused ja motivatsiooni kui käitumise mõjutegurid sobivate sekkumiste tüüpidega (Michie, 2011). Ühtlasi on COM-B/BCW mudelit ka varem küberturvalise käitumise sekkumiste analüüsimiseks kasutatud: nt leidsid van Steen *et al.* (2020) riiklikes küberturvalisuse kampaaniates kasutatud sekkumiste analüüsis, et liiga sageli panustavad tegevused inimeste teadmiste parandamisele, millest aga ei piisa kõigi kolme käitumise mõjuteguri mõjutamiseks.

COM-B/BCW mudeli kolm põhikomponenti – võimekus (ingl *capability*), võimalused (ingl *opportunity*) ja motivatsioon (ingl *motivation*) – jagunevad kõik omakorda veel kaheks alakategooriaks (vt Joonis 1).



Joonis 1. Käitumist mõjutavad tegurid COM-B mudeli järgi. Allikas: Anni Kurmiste Michie *et al.* (2011) põhjal

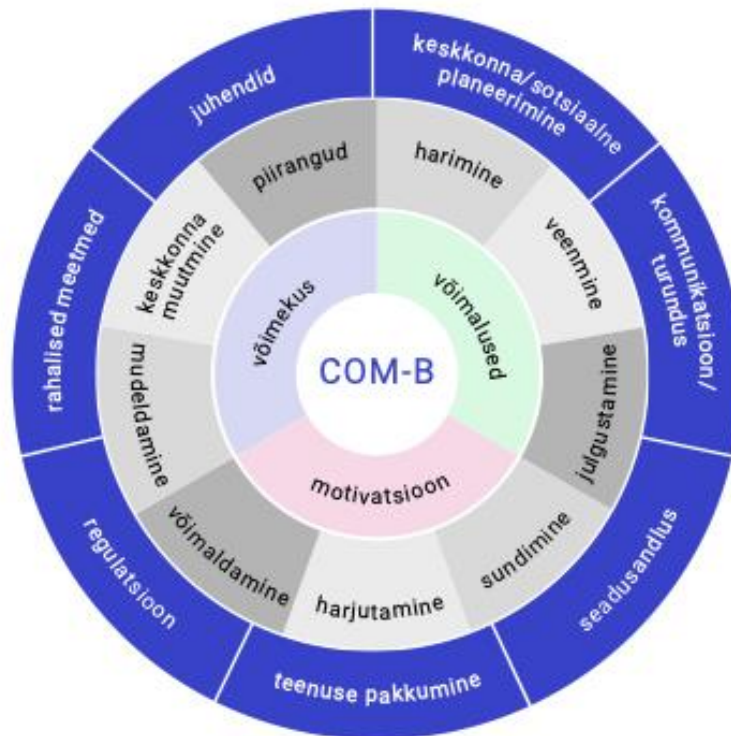
Võimekus jaguneb psühholoogiliseks võimekuseks (inimese teadmised, arusaamine, kognitiivne võimekus) ja ka füüsiliseks võimekuseks (praktilised ja tehnilised oskused/võimed). Nt võib psühholoogiline võimekus tähendada teadlikkust küberturvalistest praktikatest või riskide mõistmist. Füüsiline võimekus aga hõlmab oskusi: nt kuidas seadistada kaheastmeline autentimine või paigaldada viirusetõrjeprogramm.

Võimalused jagunevad sotsiaalseteks ja füüsilisteks võimalusteks. Sotsiaalsed võimalused tähendavad sotsiaalset survet, norme ja teiste inimeste mõju, mis võivad käitumist toetada või takistada (nt töökollektiivi või sõprade suhtumine küberturvalisusesse). Füüsilised võimalused tähendavad väliskeskkonda ja ressursse, nt kas inimesel on ligipääs vajalikele tehnilistele/tehnoloogistele vahenditele või kas keskkond, kus inimene toimib, seab talle mingisuguseid piiranguid (nt töö on kohustus kasutada VPN-i vms).

Motivatsioon jaguneb automaatseks ja refleksiivseks. Automaatne motivatsioon põhineb emotsioonidel, harjumustel ja automaatsetel reaktsioonidel, mis toimuvad ilma teadliku kaalumiseta: nt harjumus kohe kõigile e-kirjas sisalduvatele linkidele klikkida või harjumus kustutada nt kõik võõralt aadressilt tulnud e-kirjad. Refleksiivne motivatsioon on aga uskumustel, väärtustel ja eesmärkidel põhinev motivatsioon, nt soov olla eeskujuks oma lastele või uskumus, et turvalised paroolid ei jääks niikuinii meelde, seega pole mõtet neid kasutada.

Käitumise muutmise ratas (ingl *Behaviour Change Wheel*, BCW, vt Joonis 2) on neil komponentidel põhinev raamistik, mis seob võimekuse, võimalused ja motivatsiooni konkreetsete sekkumistüüpidega, mis iga komponendi mõjutamiseks kõige paremini sobivad, nt koolitused võimekuse parandamiseks või preemiad motivatsiooni tõstmiseks.

Michie jt (2013) käitumise muutmise tehnikate (ingl *Behaviour Change Techniques, BCT*) taksonoomia täiendab neid sekkumiste tüüpe, pakkudes konkreetseid tehnikaid sekkumiste rakendamiseks. Nt kui psühholoogilise võimekuse parandamiseks sobivad BCW järgi sekkumistüübina koolitused, siis täpsetest käitumise muutmise tehnikatest võib koolitustel kasutada informeerimist käitumise tagajärgedest.



Joonis 2. Käitumise muutmise ratas. Allikas: autorite koostatud Michie *et al.* (2011) põhjal

5.1. Eesti elanike küberturvalise käitumise parandamiseks sobivad sekkumised

Järgnevalt toome veelkord välja peatükis 2.5 käsitletud ajendid, mis panevad Eesti inimesi kas küberturvaliselt või vastupidi, küberhaavatavalt käituma, ning analüüsime, kuidas sihivad Eestis juba rakendatavad praktikad neid ajendeid. Samuti toome välja, millised süstemaatiliselt kirjandusülevaatest selgunud käitumist püsivalt mõjutavad sekkumistüübid nende Eesti elanike puhul oluliste ajendite mõjutamiseks sobivad ning mida võiks Eestis veel lisaks teha, et küberturvalist käitumist edendada.

Küberturvalise käitumise ajend: hirm kaotada raha/andmed/identiteet/privaatsus

Näitlikustavad tsitaadid

.../ et oma rahast mitte ilma jääda ja oma isikust [intervjueeritav peab ilmselt silmas digitaalselt identiteeti] mitte ilma jääda, siis sellele [küberturvalisusele] peab üha rohkem ja rohkem ja rohkem rõhku panema.

.../ sinu tegevustest jäävad jäljed maha ja sa ei taha ometi, et need asjad kuhugi hulkuma lähevad /.../. Ma ei tea, sa oma asju ju hoiad, samamoodi pead ju oma andmeid [internetis] ka hoidma.

COM-B elemendid

Refleksiivne motivatsioon: inimestel on motivatsioon tegutseda ohtude vältimiseks, mitte automaatse harjumuse või välise surve tõttu. Eesmärgistatud käitumine, mida suunavad uskumused käitumisviisi tagajärgede kohta.

Psühholoogiline võimekus: inimestel on teadmised ja arusaam võimalikest riskidest, mis võivad realiseeruda ja mille eest tuleb end hoida.

Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?

Meedia vahendusel jagatakse lugusid sellest, kuidas inimesed on küberturvalisuse põhitõdesid eiranud ja nt kelmuse ohvriks langenud või on nende konto häkitud. Selliste lugude eesmärk on näidata, kui kergelt võib midagi halba juhtuda ja kuidas tuleks internetis toimetades ettevaatlikum ning tähelepanelikum olla.

Ka küberturvalisusalastel koolitustel räägitakse mõnikord hoiatavalt reaalelulistest juhtumitest. Selline info aitab inimestel teadvustada riske.

Lisaks tõstab teadlikkust reaalistest riskidest ka erinevate turvahoiatuste/meeldetuletuste saamine (nt saadakse teenusepakkuvalt/rakenduselt sõnum, et inimese paroolid võivad olla osalised andmelekkes).

Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?

- 1) Tagasisidestatud kaugmonitoorimine sisuliselt adresseerib, sest põhineb käitumise muutmise tehnikatel (tagasisidestamine ja monitoorimine), mis sobivad refleksiivse motivatsiooni mõjutamiseks: inimesed saavad teadlikumaks oma tegelikust käitumisest, selle tagajärgedest ning sellest, kas see vastab eesmärkidele. Teisalt, nagu ptk-s 4 väja tõime, oleks sellist sekkumist küberturvalisuse valdkonnas väga keeruline ja kulukas rakendada. Seda saaks teha vaid RIA ja pankade või telekommunikatsiooniettevõtete koostöös ning küberhügieeni saaks distantisilt monitoorida ainult teenusepakkuja, mis muudaks sekkumise rakendamise veelgi keerukamaks (mh privaatsuse küsimus). Ka ei pruugiks inimeste motivatsioon küberturvalisuse valdkonnas (erinevalt tervisevaldkonnast, kus isiklik tajutav kasu on suurem) sellises sekkumises osaleda olla eriti kõrge.
- 2) Mitme teooria mudelil (MTM) põhinevad sekkumised käitumise muutmiseks adresseerivad seda ajendit, sest refleksiivset motivatsiooni on võimalik mõjutada just hariduslike ja veenmise sekkumistüüpidega, milleks sobivaid käitumise muutmise tehnikaid MTMil põhinevad sekkumised sisaldavad (plusside ja miinuste kaalumise, teave mõjude kohta, endasse uskumine, negatiivsete emotsioonide vähendamine, käitumise harjutamine, sotsiaalne tugi). Küberturvalisuse valdkonnas piirab rakendamist samas see, et tervet laia avalikkust poleks võimalik sekkumisse hõlmata ning pole ka teada, kas sekkumise üksikuid elemente rakendades oleks see sama tõhus.
- 3) Küberturvalisuse valvurid vanemaaliste kogukondades ja Neljakordne „E” lähenemisviis tõhusa küberhügieeni tagamiseks on sekkumised, mis samuti seda ajendit adresseerivad. Mõlemad

sekkumised põhinevad teadmiste parandamisel, mis sobivad nii psühholoogilise võimekuse kui refleksiivse motivatsiooni mõjutamiseks. Võimalik küberturvalisuse valdkonnas rakendada koostöös teiste osapooltega (nt raamatukogud, kõrgkoolid).

Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?

Kas mingeid sihtrühmi on eriti oluline silmas pidada?

Arvestades, et hirm kaotada oma raha/andmed/identiteet/ privaatsus oli üks peamisi ajendeid küberturvaliseks käitumiseks, mida intervjueeritavad välja tõid, võib öelda, et Eesti elanikud teavad ja teadvustavad erinevaid küberriske. Inimeste informeerimine ohtudest on küll oluline, eriti kuna ohud on pidevas muutumises, kuid teavitustöös tuleb rohkem tähelepanu suunata ka sellele aspektile, et inimesed küll teavad riske, ent ei usu sageli, et just nende endiga midagi juhtub, mistõttu ei rakenda nad oma teadmisi alati praktikas ega ole piisavalt ettevaatlikud. Vt allpool soovitusi selles osas, mida teha, et võidelda uskumusega, et „minuga ei juhtu mitte midagi“.

Küberturvalise käitumise ajend: **kohustus järgida küberturvalisi praktikaid**

Näitlikustav tsitaat

Mina mõtlen või rohkem tegelen sellega [küberturvalisusega] siis, kui mind sunnitakse – peamiselt lihtsalt sellepärast, et töö on sageli automaatselt rangemad nõuded. Ja siis ma lihtsalt teen nii, nagu vaja.

COM-B element

Füüsilised võimalused: mida välised tegurid ja keskkond võimaldavad või mitte. Siinkohal näide töökohal seatud kohustustest, piirangutest ja nõuetest, mis panevad inimesi käituma küberturvalisemalt.

Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?

Osal töökohtadest on selged reeglid, kuidas töökeskkonnas ja töökoha kaudu saadud seadmetes tuleb käituda, millised on küberturvalise käitumise põhiprintsiibid, mida tuleb rakendada jne. Sageli on seadmetes juba vaikimisi aktiveeritud tehnoloogilised lahendused, mis toetavad küberturvalisust (nt kaheastmeline autentimine). Töoarvutis on seadistused sellised, et pole võimalik külastada ebaturvalisi veebilehti, laadida ise alla rakendusi, tarkvara uuendatakse automaatselt jne.

Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?

Ei, ükski kirjandusülevaate käigus leitud sekkumistest/tehnikatest ei hõlmanud füüsiliste võimaluste mõjutamist. Füüsiliste võimaluste mõjutamiseks tuleb muuta keskkonda, piirata (nt ebaturvalisi) võimalusi või lisada keskkonda küberturvalise käitumise soodustajaid, nt meeldetuletusi. Vt soovitusi järgmisel real.

Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?

Kas mingeid sihtrühmi on eriti oluline silmas pidada?

Tööandjad saavad veelgi rohkem küberturvalisusele tähelepanu pöörata. Nt koostöös RIA-ga või ITL-iga saab rohkem keskenduda sellele, et mitte mõjutada vaid inimestele füüsilist võimekust (pannes seadmete kasutamisevõimalustele piiranguid vms), vaid korraldada töötajaskonnale ka harivaid, interaktiivseid küberturvalisuse koolitusi, küberõppusi ja -teste jms. Niiviisi saab mõjutada ka inimeste psühholoogilist võimekust ja motivatsiooni, mitte panna neid küberturvalisemalt käituma ainuüksi läbi kohustuse.

Küberturvalise käitumise ajend: **toetavad tehnilised/tehnoloogilised lahendused**

<p>Näitlikustavad tsitaadid</p>	<p><i>Selles suhtes [käitun] turvalisemalt küll, et nüüd on üsna kohustuslik see, et sul peab olema igal pool kaheastmeline tuvastus. /.../ varasemalt ma ei kasutanud seda üldse.</i></p> <p><i>Tugevate paroolide peale olen ka järjest üle läinud, jah. Nii nagu nutiseadmed seda võimaldavad, et nad valivad automaatselt mingisuguse tugeva parooli.</i></p>
<p>COM-B element</p>	<p>Füüsilised võimalused: põhineb väliskeskkonna võimalustel või nõuetel (millised toetavad lahendused üldse eksisteerivad).</p>
<p>Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?</p>	<p>Eksisteerivad toetavad tehnilised/tehnoloogilised lahendused nagu paroolihaldur turvaliste paroolide genereerimiseks ja haldamiseks, viirusetõrjeprogrammid jms. Paljud veebikeskkonnad ja rakendused on juba ülesehitatud nii, et seal saab kasutada vaid turvalist parooli või on ette nähtud kaheastmelise autentimise rakendamine.</p> <p>Erinevad infoallikad (juhendid, koolitused, ennetusportaal itvaatlik.ee jne) viitavad ka toetavatele lahendustele, mida inimesed võiksid rakendada, et oma küberturvalisust suurendada. Samas on kitsaskohaks see, et olgugi et sellised turvalisust toetavad lahendused eksisteerivad, takistab mugavus/harjumus inimesi neid lahendusi kasutamast.</p>
<p>Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?</p>	<p>Ei, ükski kirjandusülevaate käigus leitud sekkumistest/tehnikatest ei hõlmanud füüsiliste võimaluste mõjutamist. Füüsiliste võimaluste mõjutamiseks tuleb muuta keskkonda, piirata (nt eaturvalisi) võimalusi või lisada keskkonda küberturvalise käitumise soodustajaid, nt meeldetuletusi. Vt soovitusi järgmisel real.</p>
<p>Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?</p> <p>Kas mingeid sihtrühmi on eriti oluline silmas pidada?</p>	<p>Küberohtude maandamiseks tuleb senisest süsteemsemalt tähelepanu pöörata teenusepakkujate poolele ja e-keskkondade ohutusele. Erasektor (telekommunikatsiooniettevõtted, pangad) ja RIA koostöös saab blokeerida kahtlasi veebilehti, piirata neile ligipääsu jms.</p> <p>Teenusepakkujate roll küberturvalisuse edendamisel peab olema süsteemsemalt läbimõeldud ja nende vastutus suurem ning seda peab toetama ka seadusandlus (nt kasutajate andmete kogumisega seotud piirangud suurkorporatsioonidele; tõhusam infovahetus erasektori ja RIA ning PPA vahel).</p>

Küberhaavatava käitumise ajend: **ohutaju puudumine naiivsusest või uskumuse tõttu, et „minuga ei juhtu mitte midagi“**

<p>Näitlikustavad tsitaadid</p>	<p><i>Ma tean, et see võib-olla ei ole hea, aga /.../ mul on natuke suva. /.../ Ma ei tunne, nagu mu informatsioon oleks nii tähtis. /.../ Väga paljud inimesed lihtsalt ei arva, et neilt on väga midagi varastada, mis on natuke minu mõtlemine ka...</i></p> <p><i>/.../ see [et internetis toimetades midagi halba juhtuks] on kuidagi nii mittekäegakatsutav. Nüüd võib-olla rohkem, aga vanasti see tunduski, et minuga seda ei juhtu. Vanuse perspektiivis ka mõeldes, et ma ju olen piisavalt tark, et aru saada nendest [küberturvalisuse] asjadest.</i></p>
--	---

COM-B element	Refleksiivne motivatsioon: inimestel puudub motivatsioon küberturvaliseks käitumiseks tulenevalt oma uskumustest käitumise tagajärgede ja riskide realiseerumise kohta.
Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?	<p>Meedia vahendusel jagatakse lugusid sellest, kuidas inimesed on küberturvalisuse põhitõdesid eiranud ja nt pettuse ohvriks langenud. Selliste lugude eesmärk on näidata, kui kergelt võib midagi halba juhtuda ja kuidas tuleks internetis toimetades ettevaatlikum ning tähelepanelikum olla.</p> <p>Ühtlasi mainisid intervjueeritavad, et mõndadel küberturvalisusalastel koolitustel, kus nad on osalenud, on räägitud hoiatavalt reaalelulistest juhtumitest.</p>
Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?	<ol style="list-style-type: none"> 1) Tagasisidestatud kaugmonitoorimine sisuliselt adresseerib, sest põhineb käitumise muutmise tehnikatel (tagasisidestamine ja monitoorimine), mis sobivad refleksiivse motivatsiooni mõjutamiseks: inimesed saavad teadlikumaks oma tegelikust käitumisest, selle tagajärgedest ning sellest, kas see vastab eesmärkidele. Teisalt, nagu ptk-s 4 välja tõime, oleks sellist sekkumist küberturvalisuse valdkonnas väga keeruline ja kulukas rakendada. Seda saaks teha vaid RIA ja pankade või telekommunikatsiooniettevõtete koostöös ning küberhügieeni saaks distantsilt monitoorida ainult teenusepakkuja, mis muudaks sekkumise rakendamise veelgi keerukamaks (mh privaatsuse küsimus). Ka ei pruugiks inimeste motivatsioon küberturvalisuse valdkonnas (erinevalt tervisevaldkonnast, kus isiklik tajutav kasu on suurem) sellises sekkumises osaleda olla eriti kõrge. 2) Mitme teooria mudelil (MTM) põhinevad sekkumised käitumise muutmiseks adresseerivad seda ajendit, sest refleksiivset motivatsiooni on võimalik mõjutada just hariduslike ja veenmise sekkumistüüpidega, milleks sobivaid käitumise muutmise tehnikaid MTMil põhinevad sekkumised sisaldavad (plusside ja miinuste kaalumise, teave mõjude kohta, endasse uskumine, negatiivsete emotsioonide vähendamine, käitumise harjutamine, sotsiaalne tugi). Küberturvalisuse valdkonnas piirab rakendamist samas see, et tervet laia avalikkust poleks võimalik sekkumisse hõlmata ning pole ka teada, kas sekkumise üksikuid elemente rakendades oleks see sama tõhus. 3) Küberturvalisuse valvurid vanemaealiste kogukondades ja Neljakordne „E” lähenemisviis tõhusa küberhügieeni tagamiseks on sekkumised, mis samuti seda ajendit adresseerivad. Mõlemad sekkumised põhinevad teadmiste parandamisel, mis sobivad nii psühholoogilise võimekuse kui refleksiivse motivatsiooni mõjutamiseks. Võimalik küberturvalisuse valdkonnas rakendada koostöös teiste osapooltega (nt raamatukogud, kõrgkoolid).
Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?	Uuringu käigus intervjueeritud inimesed leidsid, et nende motivatsiooni küberturvalisusele rohkem tähelepanu pöörata suurendaks reaalne eluline näide ehk isiklik kogemus küberintsidendiga või kellegi teise (sh lähedase) kogemusloost osa saamine. Seega võiks olemasoleva praktika rakendamist jätkata ehk jagada meedias ja ka koolitustel reaalelulisi lugusid juhtumitest, kus kellegagi on internetis toimetades ohtusid eirates midagi halba

<p>Kas mingeid sihtrühmi on eriti oluline silmas pidada?</p>	<p>juhtunud. Seejuures on oluline silmas pidada, et eri sihtrühmade suunal (nt eri vanuses inimesed; ettevõtjad jne) võiks kogemuslugude levitamisel kõneisikuks olla keegi, kellega vastava sihtrühma esindaja suudab samastuda ja/või kes on tema jaoks autoriteet (nt noorte puhul suunamudijad, ettevõtjatele teine ettevõtja).</p> <p>Meediakajastuse puhul peab silmas pidama, et kui jagatakse infot levinud petuskeemidest ja inimestega juhtunust, siis ei pruugi olla hea pea alati rõhutada, et ohver oli nt vanemaealine isik või vene emakeelega inimene jne. Selline profiilide esile tõstmine mitmetes lugudes pika aja jooksul võib süvendada teistes sotsiaalsetes gruppides usku, et nad on väljaspool ohtu ja suudavad riske vältida¹⁴. Ka intervjuudest ilmnes muuhulgas, et levinud on arvamus, et küberpettuste ohvriks langevad pigem vanemad inimesed, kes on vähem teadlikud ja vähemate oskustega.</p> <p>Arvestades, et uskumus, et „minuga ei juhtu mitte midagi“ võib olla seotud ka oma küberturvalisusalaste teadmiste üle hindamise ja sellest tingitud võltsenesekindlusega (tõenäolisem noorte puhul), võib kasu olla ka ettehoiatamata toimuvatest küberõppustest või -testidest, kus mingi sihtrühma (nt õpilased) teadlikkus ja tähelepanelikkus pannakse reaajas proovile (vt selle kohta ka täpsemalt ptk 3.4.1).</p>
---	---

<p align="center">Küberhaavatava käitumise ajend: mugavus/laiskus/hooletus/väsimus/kiirustamine pärsib küberturvalist käitumist¹⁵</p>	
<p>Näitlikustavad tsitaadid</p>	<p><i>Parooli asjades ma ei ole eriti eeskujulik. Enamasti on üks või kaks parooli, mida ma kasutan, mis ma tean, et on väga vaele, aga lihtsalt nii hea lihtne on. Eriti siis, kui sa teed kasutaja, mida sa tead, et sa kasutad ainult ühe korra või kaks korda.</i></p> <p><i>Kaheastmelise autentimise puhul tunnistan tõesti üles, et ei kasuta, sest vastus on: tüütu. Sa tahad midagi ruttu ja siis hakkab pihta /.../ See on lõivu maksmine mugavusele.</i></p> <p><i>Mingil hetkel võib-olla tähelepanu hajub või sa oledki juba liiga kaua aega internetis olnud. Enda puhul võin öelda, et see oli ikkagi enamasti tähelepanematuses [et ei olnud hoolas].</i></p>
<p>COM-B element</p>	<p>Automaatne motivatsioon: käitumist juhivad impulsid, emotsioonid, (harjumused või mugavus) ja seda mõjutab ka nt väsimuse tõttu vähenenud eneseregulatsioon.</p>
<p>Kas olemasolevad sekkumised/praktikad</p>	<p>Eksisteerivad küberturvalist käitumist toetavad tehnilised/tehnoloogilised lahendused (vt üle-eelmine ajend, mida</p>

¹⁴ Vt ka esinduslikkuse heuristik – kui ohvrit ainult mingi kindla stereotüübina kujutada, muutub see kõige esinduslikumaks näiteks ja hakkab tunduma, et teisi gruppe see ei puuduta (Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, 185(4157), 1124–1131. <https://doi.org/10.1126/science.185.4157.1124>)

¹⁵ Oleme siinkohal liitnud üheks ajendiks „mugavus ja laiskus pärsib küberturvalist käitumist“ ning „hooletus/väsimus/kiirustamine tingib küberhaavatava käitumise“, kuna neid on COM-B elementide ja võimalike sekkumiste vaates praktilisem analüüsida üheskoos.

adresseerivad seda ajendit? Millised?

käsitlesime). Nt osa teenuste/rakenduste puhul on juba vaikimisi eeldus, et sisselogimine on kaheastmelise autentimisega. Samuti paroolihaldur kui vahend turvaliste paroolide genereerimiseks ja haldamiseks, ilma et neid peaks kõigi eri kontode puhul eraldi meelde jätma (seega inimene ei saa väita, et ta ei saa keerukaid paroole kasutada, kuna need ei jää tal meelde). Ekraanilukustus jms meetmed.

Seda ajendit adresseerib ka see, kui eksisteerivad kohustuslikud turvapraktikad (nt töökohal), mis ei võimalda mugavuse või laiskuse tõttu hooletumalt käituda. Ühes keskkonnas kohustuse tõttu rakendatavad käitumispraktikad võivad seejuures saada harjumuseks ja kanduda üle ka teistesse keskkondadesse ehk inimese küberkäitumine muutub tervikuna turvalisemaks (nt nii töö- kui eraseadmetes).

Kas mõni kirjandusülevaate käigus leitud sekkumistest/ tehnikatest võiks seda ajendit adresseerida? Kuidas?

1) Mitme teooria mudelil põhinevad sekkumised sobivad osaliselt, sest sisaldavad mh ka käitumise harjutamist, mis sobib automaatse motivatsiooni mõjutamiseks. Samas piirab sekkumise rakendamist küberturvalisuse valdkonnas see, et tervet laia avalikkust poleks võimalik sekkumisse hõlmata ning pole ka teada, kas sekkumise üksikuid elemente rakendades oleks see sama tõhus.

2) Sekkumised, mis põhinevad preemiatel (nt eespool toodud sekkumine, kus jagati preemiaid prügi sorteerimise eest) võivad sobida automaatse motivatsiooni mõjutamiseks. Küberturvalisuse valdkonnas sekkumise rakendamisel on selle tugevus, et seda on võimalik rakendada, hõlmates korraga võrdlemisi laia sihtrühma. Samas ei saa RIA kui riigiamet olla rahaliste preemiate pakkuja, sest see poleks kohane. Auhindade loosimist, kollektiivseid mängulisi ja võistluslikke väljakutseid saaksid rakendada teised küberturvalisuse edendamise seotud osapooled (nt pangad, telekommunikatsiooniettevõtted).

Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?

Kas mingeid sihtrühmi on eriti oluline silmas pidada?

Küberohtude maandamiseks on oluline senisest süsteemsemalt tähelepanu pöörata ka teenusepakkujate poolele ja e-keskkondade ohutusele. Teenusepakkujate roll küberturvalisuse edendamisel peab olema seejuures süsteemsemalt läbimõeldud ja nende vastutus suurem ning seda peab toetama ka seadusandlus.

Ka koostöö nt tööandjate ja haridusasutustega kui keskkondadega, kus inimesed palju viibivad, võib olla tulemuslik, kui neis keskkondades suudetakse inimestel tekitada küberturvalisi harjumusi, mis kanduvad edasi ka igapäevaellu.

Arvestades, et automaatse motivatsiooni mõjutamiseks on sobilikud ka preemiatel põhinevad sekkumised, siis võiks kaaluda materiaalsete stiimulite abil inimeste käitumise mõjutamist (nt preemiad, auhinnad, kollektiivsed väljakutsed, nagu oli nt rahatarkuse mäng jms).

Küberhaavatava käitumise ajend: **küberturvalisusalased teadmised on puudulikud, ülehinnatud või praktikas rakendamata**

<p>Näitlikustav tsitaat</p>	<p><i>Ma tean [küberturvalisest käitumisest] üht-teist, aga kindlasti mitte piisavalt. Võib-olla ongi mingeid asju, mida ma üldse ei teagi veel ja ei oska aru saada, et ma ei tea.</i></p> <p><i>Ma arvan, et ma mingil määral olen [keskmisest küber]teadlikum, aga samas ma ei ole kindel, kas ma ka igapäevaselt seda teadlikkust kasutan, sest ikkagi on mitu korda olnud see... Just näiteks Facebooki Marketplace'iga need skämmerid, kelle otsa olen sattunud.</i></p>
<p>COM-B element</p>	<p>Psühholoogiline võimekus: inimestel puuduvad teadmised või arusaamine küberturvalisusest ja olulistest küberturvalisusalastest käitumispõhimõtetest.</p>
<p>Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?</p>	<p>Üldine teavitus- ja ennetustöö (info jagamine massi- ja sotsiaalmeedias, koolitustel, töökohtadel ning haridusasutustes jms)</p>
<p>Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?</p>	<ol style="list-style-type: none"> 1) Tagasisidestatud kaugmonitoorimine sisuliselt adresseerib, sest põhineb käitumise muutmise tehnikatel (tagasisidestamine ja monitoorimine), mis sobivad refleksiivse motivatsiooni mõjutamiseks: inimesed saavad teadlikumaks oma tegelikust käitumisest, selle tagajärgedest ning sellest, kas see vastab eesmärkidele. Teisalt, nagu ptk-s 4 välja tõime, oleks sellist sekkumist küberturvalisuse valdkonnas väga keeruline ja kulukas rakendada. Seda saaks teha vaid RIA ja pankade või telekommunikatsiooniettevõtete koostöös ning küberhügieeni saaks distantsilt monitoorida ainult teenusepakkuja, mis muudaks sekkumise rakendamise veelgi keerukamaks (mh privaatsuse küsimus). Ka ei pruugiks inimeste motivatsioon küberturvalisuse valdkonnas (erinevalt tervisevaldkonnast, kus isiklik tajutav kasu on suurem) sellises sekkumises osaleda olla eriti kõrge. 2) Sekkumised, mis sarnaselt individuaalselt kohandatud motiveerivale suuhügieeniprogrammile hõlmavad teadmiste kujundamist, sobivad psühholoogilise võimekuse parandamiseks. Küberturvalisuse valdkonnas tuleks samas sekkumise rakendamiseks valida kitsam sihtrühm kui kogu elanikkond või suurem osa sellest, sest vastasel juhul on tegu liiga ressursimahuka tegevusega. Küll aga saaks sekkumist rakendada kitsamas sihtrühmas: nt koostöös ettevõtetega, Väarikate Ülikoolidega, vabaühendustega jms. 3) Küberturvalisuse valvurid vanemaealiste kogukondades ja Neljakordne „E” lähenemisviis tõhusa küberhügieeni tagamiseks on sekkumised, mis samuti seda ajendit adresseerivad. Mõlemad sekkumised põhinevad teadmiste parandamisel, mis sobivad nii psühholoogilise võimekuse mõjutamiseks. Võimalik küberturvalisuse valdkonnas rakendada koostöös teiste osapooltega (nt raamatukogud, kõrgkoolid).
<p>Millised on lüngad küberturvalist käitumist edendavate sekkumiste</p>	<p>Puudulike teadmiste korral küberturvalisusalase (lisa)info jagamine sihtrühma poolt eelistatud viisil (nt noortele pigem sotsiaalmeedia kaudu levitavate lühivideote vahendusel ning (kõrg)kooli kaudu;</p>

pakkumises ehk mida tuleks lisaks teha?	eakamatele personaalne nõustamine või õpitoad + infovoldikute saatmine jne).
Kas mingeid sihtrühmi on eriti oluline silmas pidada?	Teadmiste ülehindamine või praktikas rakendamata jätmine on miski, mis on tõenäoliselt vähemalt osaliselt seotud uskumusega, et „minuga ei juhtu mitte midagi“. Selle ajendi adresseerimiseks võiks toimida reaaleluliste näidete pakkumine inimestele (nt stimuleeritud isiklik kogemus küberintsidendiga küberõppuse või -testi raames või teiste inimeste kogemuslugude jagamine).

Küberhaavatava käitumise ajend: **küberturvalist käitumist takistab sotsiaalne surve**

Näitlikustav tsitaat	<i>./.../ mis on tekitanud muret, on TikTok. Seda ei soovitata kasutada, kuna on mingeid kahtlusi infolekke kohta, aga samas see on selline platvorm, mis minuealiste seas on väga populaarne ja väga oluline. Ma ikkagi kasutan seda –see võib-olla on selline asi, mis tekitab natuke muret.</i>
COM-B element	Sotsiaalsed võimalused: käitumine mõjutatud sotsiaalsest survest, teistest inimestest, sotsiaalsetest normidest.
Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?	Spetsiaalselt sellele ajendi adresseerimiseks mõeldud sekkumisi/praktikaid ei ole.
Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?	<ol style="list-style-type: none"> 1) Mitme teooria mudelil põhinevad sekkumised osaliselt sobivad, sest sisaldavad ka sotsiaalse toe elementi, nt pere, sõbrad ja tutvusringkond, kes on soovitud käitumise suhtes toetavad; mentorlus või tugigrupid; käitumist toetava väljakutsega ühiselt liitumine. Samas piirab sekkumise rakendamist küberturvalisuse valdkonnas see, et tervet laia avalikkust poleks võimalik sekkumisse hõlmata ning pole ka teada, kas sekkumise üksikuid elemente rakendades oleks see sama tõhus. 2) Sekkumised nagu küberturvalisuse valvurid vanemaealistes kogukondades, kus on fookuses ka küberkäitumise teemade normaliseerimine teatud kogukonnas, sihib samuti sotsiaalsete võimaluste loomist ja sobiks seega selle ajendi adresseerimiseks.
Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?	Vajadus lähenemise järele, kus rakendataks mingi sihtrühma põhist vastastikuse õppimise põhimõtet (nt kogukonnapõhine lähenemine) või kõneisikuid (nt suunamudijaid), kes on konkreetses sihtrühmas populaarsed ja autoriteetsed. Oluline on, et küberturvalist käitumist esitletaks inimestele justkui uhkuse ja kuuluvuse sümbolina ning millegi atraktiivsena, et innustada inimesi seeläbi oma turvalisusele rohkem tähelepanu pöörama.
Kas mingeid sihtrühmi on eriti oluline silmas pidada?	Oluline siinkohal silmas pidada noori, kellel on tihti kõrge kuuluvusvajadus ning kes on vastuvõtlikumad eakaaslaste sotsiaalsele survele. Arvestades, et intervjuudest ilmnis päris palju ka seda, et sotsiaalsed võimalused vastupidiselt soodustavad küberturvalist käitumist (nt peres on küberturvalised harjumused; nooremad sugulased juhendavad vanemaid; kolleegid motiveerivad turvalisemalt

käituma), on ühtlasi oluline soosida sellist käitumist ehk pöörata negatiivne sotsiaalne surve n-ö ümber (nt sarnased kampaaniad nagu Maanteeameti "SÕBER ei lase purjus SÕPRA rooli").

Küberhaavatava käitumise ajend: **puuduvad võimalused kasutada turvalisi lahendusi/seadmeid**

Näitlikustavad tsitaadid

Ma tuleks siin piraatluse juurde tagasi. Minu puhul on lihtsalt see, et meedia [tarbimine] maksab. Kahjuks ei ole alati seda, mille eest minna seda [sisu], kas siis Netflixist vaatama, kinno, mis iganes, onju. Minu puhul on lihtsalt see, et ma olen teadvustanud, kuidas nendel lehtedel [piraatlusega tegelevatel saitidel] navigeerida – pigem on see, et ma olen õppinud selles keskkonnas eksisteerima /.../ Aga minu jaoks on see... ma ei tea kui palju kalkuleeritud risk, aga teadlik risk.

Oled sa siis ülikooliõpilane või midagi muud sarnast – raamatud on röögatult kallid, eriti veel akadeemiline kirjandus. Kui sa saad selle [vajaliku raamatu] kuskilt... ma ei tea, kunagi oli Z-library. /.../ Kui sul on võimalus alla laadida tasuta, siis sa kasutad seda. Aga see tuleb riskiga, et sa laed alla veel midagi peale selle kirjavara.

COM-B element

Füüsilised võimalused: põhineb väliskeskkonna võimalustel ja nõuetel (pole ligipääsu turvalistele lahendustele/seadmetele, sest puuduvad ressursid).

Kas olemasolevad sekkumised/praktikad adresseerivad seda ajendit? Millised?

Kohati on teatud keskkondades inimestele siiski tagatud vajalikud ligipääsud/seadmed (nt töökohtadel antakse kaitstud/seadistatud tööarvuti või haridusasutustes õpilastele ligipääs akadeemilistele andmebaasidele). Ka raamatukogude (nt Rahvusraamatukogu) kaudu on võimalik registreerunud lugejatel saada ligi teatud andmebaasidele. Lisaks toimub võitlus netipiraatlusega (nt piraatsisu levitavate lehtede blokeerimine).

Kas mõni kirjandusülevaate käigus leitud sekkumistest/tehnikatest võiks seda ajendit adresseerida? Kuidas?

Ei, füüsilisi võimalusi mõjutavaid sekkumisi/tehnikaid me kirjandusülevaate käigus ei leidnud. Füüsiliste võimaluste mõjutamiseks tuleb muuta keskkonda, piirata ebaturvalisi võimalusi, muuta turvaliste võimaluste kasutamine kergeks ja ligipääsetavaks, lisada keskkonda küberturvalise käitumise soodustajaid, nt meeldetuletusi.

Millised on lüngad küberturvalist käitumist edendavate sekkumiste pakkumises ehk mida tuleks lisaks teha?

Ebaturvaliste võimaluste kasutamise piiramine (nt piraatlehtedele ligipääsu blokeerimine) kombineerituna turvaliste lahenduste kättesaadavamaks muutmisega (nt ligipääs e-raamatutele, õppematerjalidele).

Kas mingeid sihtrühmi on eriti oluline silmas pidada?

Noored (õpilased) on oluline sihtrühm, kellel on reeglina piiratud rahalised võimalused, kuid samas suur vajadus õppematerjalide ja meelelahustusliku sisu järele, mis võib viia ebaturvalise käitumiseni.

6. Järeldused ja soovitused

Järgnevalt toome välja siinse uuringu peamised järeldused Eesti elanike küberteadlikkuse ja -käitumise kohta ning neist järeldustest tulenevad soovitused küberturvalise käitumise edendamiseks. Oleme järeldused ja soovitused jaotanud kolme ossa vastavalt sellele, kas soovitused keskenduvad:

- ennetus- ja teavitustegevustele, mida RIA saab ise laiema avalikkuse suunal ellu viia;
- ennetus- ja teavitustegevustele, mida RIA saab ellu viia koostöös partneritega nagu tööandjad ja haridusasutused;
- ennetus- ja teavitustegevustele, mida RIA saab ellu viia koostöös teenuseomanike ja teenusepakkujatega.

Ennetus- ja teavitustegevused, mida RIA saab ise laiema avalikkuse suunal ellu viia

Nr	Järeldus	Soovitus
1.	Inimeste peamine ajend küberturvaliseks käitumiseks on hirm kaotada oma raha, andmed, identiteet või privaatsus. Intervjuudest ilmnes, et inimesed on just internetipankades ja e-poodides toimetades teistest keskkondadest ettevaatlikumad, sest seal on nende jaoks rohkem kaalul. Sisuliselt on need intervjuueeritavad kalkuleerinud riske ja leidnud enda jaoks vastuvõetava tasakaalu. See tähendab, et inimestel on küberturvalisusalased teadmised (psühholoogiline võimekus) olemas ja neid rakendatakse praktikas valikuliselt – mingite tegevuste käigus rohkem, teisel juhul vähem (automaatne/refleksiivne motivatsioon), mõne vastaja puhul riskipõhiselt.	<p>Õpetada tavakasutajaid mõistma oma riskiprofiili ja võtma kasutusele kohaseid küberturvalisuse praktikaid ka väljaspool pankade ja e-poodide konteksti, kus osa inimesi juba oskab riske meeles pidada ja ära tunda. Kasutada seejuures lihtsaid, tavainimesele arusaadavaid sõnumeid ja vältida tehnoloogia ning riskijuhtimise termineid. Nt kampaania "Hoiu, mis oluline":</p> <ul style="list-style-type: none"> - Mis on kaalul/ohus (nt olulisemate meilikontode puhul nii nende kättesaadavus kui ka seal olevad andmed; rakendusega geolokatsiooni jagamisel kasutaja privaatsus, pangaandmete või pangakontole ligipääsu jagamisel raha jne); - Mida tuleks kaitsta ehk mis on kasutaja jaoks kõige olulisem (nt ligipääs oma kontodele ja kasutaja andmed, mis võimaldavad ligipääsu mitmele teenusele sh nii ID-kaart kui ka Google, sotsiaalmeediarakendused jne); - Mis on kohane kaitsemeede (nt mitmefaktoriline autentimine olulisemate kontode puhul, ootamatu e-kirja puhul saatjaga selle õigsuse kontrollimine alternatiivse suhtluskanali (nt telefon) kaudu jms).

Selliste sõnumite puhul on suur väärtus võrdlusel (mingite teenuste/tegevuste puhul on turvalisus olulisem ja seega ka tehakse selle nimel rohkem, nagu töid välja ka intervjueritavad), samas tähendab see, et kommunikatsioonis öeldakse välja, et mõned teenused on madalama riskitasemega ning kampaania korraldaja peab olema valmis sellist sõnumit aktsepteerima.

Kasutada küberturvalise käitumise edendamisel kombineeritult inimeste sisemist motivatsiooni mõjutavaid sekkumisi (nt kogemuslugude jagamine; enda küberturvalisusalaste teadmiste testimise võimalus) ja ka väliseid stiimuleid (nt auhinnad või soodustused, kollektiivsed võistluslikud väljakutsed nagu Swedbanki rahatarkuse mäng vms). Väliste stiimulite kasutamisel võib seejuures eeskuju võtta ptk-s 4 välja toodud sekkumisest „Preemiad prügi sorteerimise eest“.

2. Üks peamisi põhjuseid, miks Eesti elanikud küberruumis baashügieeni ei järgi, on tingitud uskumusest „minuga ei juhtu mitte midagi“.

Jätakuvalt jagada (sotsiaal)meedias ja ka küberturvalisusalastel koolitustel reaalelulisi lugusid juhtumitest, kus kellegagi on internetis toimetades ohtusid eirates midagi halba juhtunud. Jälgida meediakajastuse puhul seejuures, et ohvritena ei kujutataks pidevalt sarnase taustaga inimesi (nt vanemaealisi, vene emakeelega inimesi, madalama haridustasemega inimesi) ning et lugude toon ja esitamiski viis oleks ligipääsetav ja mõistetav kõigile eagruppidele.

Pakkuda inimestele võimalust teha digitaalne küberturvalise käitumise test (sarnaselt digitestiga, mida kohaldada vastavalt tavakasutajale), mille läbimise järel saab igaüks isikliku küberturvalise käitumise võrdluse ja riskiprofiili, mis põhineb testi sisendil. Oluline on seejuures mängulisus – inimene saab teada, milline on tema küberteadlikkus; milline on see võrdluses keskmisega; millistel teemadel/tegevustes on ta üle keskmise eeskujulik; millistest teemadest oleks tal vaja seoses küberturvalisusega rohkem teada jne. Testi läbimise järel saab inimene individuaalsele sisendile tuginevad soovitused ja materjalid või viited, mida ta peaks veel silmas pidama, et enda küberhügieeni parandada. Selline lahendus võimaldaks inimesel üheltpoolt saada hinnang oma

	<p>valmidusele küberohtusid ära tunda ja vältida ning teisalt annaks ka praktilise sisendi edasisteks tegevusteks.</p>
<p>3. Kohati paneb inimesi, sh eriti noori küberohtusid eirama ja ebaturvalisemalt käituma ka sotsiaalne surve.</p>	<p>Rakendada küberturvalise käitumise edendamisel kogukonnapõhist lähenemist (vt ka ptk-s 4 välja toodud sekkumist, kust vanemaealistes kogukondades kasutati küberturvalisuse valvureid) või kõneisikuid ja kanaleid, kes/mis on teatud sihtrühmas populaarsed ja autoriteetsed ning aitavad levitada sõnumit, et hea küberhügieen on äge, nutikas ja väärtust loov. Noorte suunal teha koostööd nt õpilasesinduste, noortekeskuste ja noorteühendustega ning ka noorte hulgas populaarsete brändide ja suunamudijatega. Vanemaealiste suunal saab lisaks kogukonnapõhisele lähenemisele teha koostööd eagrupidis populaarsete tele- või raadiosaadetega (nt „Õnne 13“, „Prillitoos“, „Päevatee“), et nende kaudu võimendada sõnumit küberturvalise käitumise olulisusest.</p> <p>Pidada seejuures silmas, et kõneisikud oleksid usaldusväärsed, pädevad teemast kõnelema ning jagaksid korrektset ja asjakohast informatsiooni. Selleks on vajalik ka kõneisikute koolitamine, nende tegevuste koordineerimine ja asjakohaste infomaterjalidega toetamine. Tasustatud kõneisikute kasutamine sõltub kampaania korraldaja võimalustest.</p>
<p>4. Eesti inimesed saavad küberturvalisuse kohta informatsiooni peamiselt massi- ja sotsiaalmeediast, aga ka teistelt inimestelt (nt pere- või sõpraderingis).</p>	<p>Jätkata ka edaspidi massi- ning sotsiaalmeedias küberturvalisusalase info jagamist (sh avalike kampaaniate raames) ning ka praktiliste, osalejaid kaasavate koolituste korraldamist ehk kombineerida sõnumi edastamiseks erinevaid kanaleid ja formaate.</p> <p>Kombineerida eelnimetatud tegevusi personaalsemate ja sihtrühmapõhiste lahendustega: kogukonnapõhised koolitused/mentorlus, personaalne nõustamine (nt juturobotiga infoliin või veebiplatvorm¹⁶; õpitoad). Kitsamas sihtrühmas saaks rakendada</p>

¹⁶ Peame siin ja edaspidi infoliinile/veebiplatvormile viidates silmas, et tehnoloogia arengut arvesse võttes, võiks makstud tasulise nõustaja asemel kasutada just tehisaru- või skriptipõhist ja stsenaariumitel baseeruvat lahendust, mida pakutakse veebi ja/või telefoni teel.

sarnast sekkumist nagu on ptk-s 4 välja toodud „Individuaalselt kohandatud suuhügieenialane programm“, mille saaks kohandada küberturvalisuse valdkonnale.

Soosida nii küberturvalise käitumise edendamiseks kui sotsiaalse sidususe suurendamiseks lähenemist, kus eakamaid inimesi toetavad küberturvalisel käitumisel info jagamise ja juhendamisega noored või teised kogukonnaliikmed (vt ka ptk-s 4 välja toodud sekkumist, kust vanemaealistes kogukondades kasutati küberturvalisuse valvureid). Tagada sellise toetava rolli tõhusaks täitmiseks ka nn tööriistakast (materjalid ja koolituspõhjad, koolitajate koolitamine, et nad teaksid, kuidas juhendada, millest rääkida jms).

5. Küberturvalisusalast informatsiooni leidub inimeste hinnangul piisavalt, mõnede jaoks on küberturvalisusalast teavet saadaval isegi tüütult palju ja see võib vähendada võimet/tahtmist infole tähelepanu pöörata. Samas on endiselt murekoht see, et asjakohane info ei pruugi alati inimestele ette sattuda ja huvi või mure korral tuleb sel juhul vajalikku teavet ise otsida. Ühtlasi on küberturvalisusalased teadmised ja õige käitumine ajas muutuvad, sest valdkond areneb kiiresti ja ka ohud on pidevas teisenemises.

Keskenduda küberturvalisusalase info levitamisel mitte ainult ohtudele, mis on seni levinum lähenemine, vaid ka küberturvalisuse positiivsele kuvandile – arukas, nutikas, atraktiivne ja väärtust loov on olla küberteadlik inimene. Uudne lähenemisnurk võib äratada ka nende inimeste tähelepanu, kellele hoiatav informatsioon on muutunud tüütavaks.

Koostada konkreetseid ja lihtsaid juhiseid (nt „Kolm sammu ID-kaardi kasutamisel“, „Mida pidada silmas e-poes osteldes“, „Keda teavitada, kui saad kahtlase kõne?“ vms) vastavalt sihtrühmale ja tehnoloogiakasutusele. Eristada seejuures küberturvalisusalase info sõnumiseades ja sisulistest (juhend)materjalides rohkem telefoni ja arvutisse puutuvat, et inimestel oleks lihtsam mõista, mida on olulisim just ühe või teise seadme puhul silmas pidada.

Levitada neid konkreetseid ja lihtsaid juhiseid mh RIA küberturvalisuse aastaraamatu avaldamise ajal, mil küberturvalisuse teema saab keskmisest enam tähelepanu ja mil juhised on ühtlasi võimalik (vähemalt osaliselt) siduda ka aastaraamatu põhiteemadega, rõhutades seejuures just värskeimat teavet ning aktuaalsemaid ohte.

Rakendada senisest enam küberturvalisusalast personaalset nõustamist (nt juturobotiga infoliin või veebiplatvorm; õpitoad), et iga inimene saaks

vajadusel küsida just seda teavet, mis teda huvitab ja mida tema vajalikuks peab. Kitsamas sihtrühmas saaks individuaalse lähenemise tagamiseks rakendada ka sarnast sekkumist nagu on ptk-s 4 välja toodud „Individuaalselt kohandatud suuhügieenialane programm“, mille saaks kohandada küberturvalisuse valdkonnale.

Tuletada inimestele järjepidevalt meelde, et kübermaailmas on kõik pidevas muutumises, mistõttu tuleb pidevalt aja ning arengutega kaasas käia. Õpetada tavakasutajaid muutuvaid olusid arvesse võttes mõistma oma riskiprofiili ja võtma kasutusele kohaseid küberturvalisuse praktikaid (vt ka 1. järeldus ja selle juurde kuuluv vastavasisuline soovitus).

6. Küberturvalisusega seotud teemad, mille kohta inimesed rohkem teavet soovivad, on eelkõige tehisaru ja selle kasutamisega seonduv, (isiku)andmete kaitsmine ja privaatsus ning ka turvaliste paroolide rakendamine. Eri sihtrühmade infovajadus võib seejuures olla erinev – kui nt noored sooviksid saada rohkem süvitsiminevat, nii-öelda edasijõudnute taseme informatsiooni, siis vanemate vanusegruppide seas on tulenevalt info üleküllusest vajadus selge ja lihtsal moel esitatud teabe järele, mis kordab üle küberturvalisuse põhitõdesid.

Rakendada senisest enam küberturvalisusalast personaalset nõustamist (nt juturobotiga infoliin või veebiplatvorm; õpitoad), et iga inimene saaks vajadusel küsida just seda teavet, mis teda huvitab ja mida tema vajalikuks peab. Kitsamas sihtrühmas saaks individuaalse lähenemise tagamiseks rakendada ka sarnast sekkumist nagu on ptk-s 4 välja toodud „Individuaalselt kohandatud suuhügieenialane programm“, mille saaks kohandada küberturvalisuse valdkonnale.

Kasutada vanemate inimeste küberturvalise käitumise edendamiseks kombinatsioonis nii lihtsa ja selge sisuga infovoldikud, mis tuletaksid inimestele meelde küberhügieeni põhimõtteid koos asjakohaste näidetega, kui ka personaalset nõustamist (nt üks-ühele nõustamised raamatukogudes, mida paljudes kohtades juba ka pakutakse, aga ka väikestes gruppides toimuvad õpitoad; „noorelt eakale“-juhendamine ja kogukondlike mentorite rakendamine nagu ptk-s 4 välja toodud sekkumine, kust vanemaealistes kogukondades kasutati küberturvalisuse valvureid).

7. Iseenda turvalisuse tagamise kõrval motiveerib inimesi küberturvalisusele rohkem tähelepanu pöörama ka eduelamus ja tunnustus õige käitumise eest. Inimeste jaoks, kes on küberohtudest märku andnud, on oluline saada tagasisidet ja tunnustust, et nende õige teguviis on aidanud ohu elimineerida.

Vaadata üle RIA ja partnerite kanalid ja protsessid, et leida senisest enam ja igakülgselt (mitte ainult tänu väljendava automaatvastusena) viise, kuidas saaks tänada/tunnustada inimesi, kes on küberohtusid märganud ja neist teada andnud. Kasutada võimalusel avalikku tunnustamist stiilis „Toomas tegi nii: Toomas on tubli ja aitas pettuse ära hoida“, mida on rakendanud ka PPA oma

kommunikatsioonis, sest see mudeldab õiget käitumist ja õpetab ka teistele, kuidas on korrektne toimida.

Tõsta laiemalt esile küberturvalist käitumist kui midagi tunnustust väärivat, nt sarnased kampaaniad nagu Transpordiameti liiklusohutuskampaania „Eesti kõige kõvem mees“.

Ennetus- ja teavitustegevused, mida RIA saab ellu viia koostöös tööandjate või haridusasutustega

Nr	Järeldus	Soovitus
8.	(Kõrg)kool on küll üks allikas, kust noored küberturvalisuse kohta informatsiooni saavad, ent intervjuude põhjal võib väita, et küberturvalisusega seonduvat käsitletakse koolis kas liiga hilja, ülemäära lihtsustatult või ebahuvitavaal moel.	<p>Lõimida küberturvalisuse edendamine süsteemsemalt haridusasutuste tegevustesse läbi sisukama teemakäsitlemise ainetundides/-kursustel. Vt seejuures ka kirjandusülevaate käigus leitud sekkumist „Neljakordne „E“ lähenemisviis tõhusa küberhügieeni tagamiseks“ (ptk 4), mis põhineb teadmiste parandamisel, sobides nii õppijate psühholoogilise võimekuse kui ka refleksiivse motivatsiooni mõjutamiseks. Õppijates teema vastu suurema huvi äratamisel ja küberturvalisuse edendamise lõimimisel haridusasutuste tegevusse võib kasu olla ka kollektiivsetest väljakutsetest, kus õpilased saavad juhendajate toel osaleda (nt küberturvalisuse teemaliste loovtööde (nt videote) konkursid / „Rakett 69“ telesaate stiilis võistlus jms).</p> <p>Koostada haridusasutuste jaoks lihtsaid ja eakohaseid küberturvalisusalaseid õppematerjale (videoloengud, tunnikavad, harjutused, (rolli)mängud jne), mida õpetajad saavad eri õppeainetes kasutada ning neist küberturvalisuse teema selgitamisel lähtuda.</p> <p>Korraldada (kõrg)koolides ettehoiatamata toimuvaid küberõppusi või -teste, et panna noorte teadlikkus ja valvsus reaalses maailmas proovile ning vältida võltsensatsioonide teket.</p>
9.	Osaliselt on inimeste (sh eriti noorte) küberhaavatav käitumine tingitud sellest, et alati pole võimalik kasutada digilahendusi, mis oleksid kontrollitud ja ohutud (nt õpingute käigus vajalike materjalide	<p>Informeerida inimesi riskidest, mis kaasnevad kontrollimata ja ebaturvaliste lahenduste kasutamisega ning muuta samal ajal turvaliste lahenduste kasutamine kättesaadavamaks (nt õpingute ajal</p>

ja programmide alla laadimine piraatlehtedelt), sest puuduvad piisavad rahalised ressursid ja nii minnaksegi teatud sisu tarbimiseks ebaturvalisemat teed.

tasuta/soodustusega ligipääs e-raamatutele, õppematerjalidele, vajalikele programmidele).

10. Töökoht on üks allikas, kust inimesed küberturvalisuse kohta informatsiooni saavad. Ühtlasi on kohustus töökeskkonnas küberturvalisi praktikaid järgida üks ajenditest, mis paneb inimesi (hoolikamalt) küberturvalisuse põhitõdesid järgima.

Pöörata töökohtadel rohkem tähelepanu inimeste küberturvaliste käitumisharjumuste kujundamisele, korraldades küberturvalisusalaseid koolitusi või rakendades muid asjakohaseid sekkumisi nagu ptk-s 4 välja toodud sekkumine „Individuaalselt kohandatud suuhügieenialane programm“, mis põhineb kognitiiv-käitumuslikel põhimõtetel ja motiveerival intervjuerimisel ning mille puhul motivatsioonisõnumite pidev kordamine viib pikaajalise käitumise muutuseni.

Tagada tööandjatele küberturvalisusalaste koolituste korraldamiseks ja asjakohase info jagamiseks igal aastal uuendatavad kvaliteetsed sisekoolituse jm infomaterjalid (slaidiesitlused, faktilised, nõuandartiklid, videokoolitused vms), mis võimaldavad tööandjatel ka küberturvalisusalast tippkompetentsi omamata teemale rohkem tähelepanu pöörata. Koostada materjalid nii, et need on kohaldatavad sektorite/töökoha profiili/ettevõtte suuruse järgi (nt 30 min ja 90 min koolituse materjalid; faktilised küberturvalisuse põhitõdedega arvutiga töötavatele/mittetöötavatele inimestele jms).

Vajadusel koolitada enne ka koolitajaid, kes asuvad sisekoolitusi läbi viima.

Korraldada töökohtadel ettehoiatamata toimuvaid küberõppusi või -teste, et panna inimeste teadlikkus ja valvsus reaalajas proovile ning vältida võltsenesekindluse teket. Informeerida ettevõtteid seejuures aktiivsemalt sellest, et RIA-l on olemas tasuta koolitus- ja testikeskkond Kübertest, millega ettevõtted saavad soovi korral liituda.

Ennetustegevused, mida RIA saab ellu viia koostöös teenuseomanike ja teenusepakkujatega

Nr	Järeldus	Soovitus
11.	<p>Eesti elanikel on küberturvalisusalased teadmised nende endi hinnangul küll olemas, kuid nende teadmiste järjepidev rakendamine igapäevases küberkäitumises võib jääda kohati puudulikuks. Toetavad tehnilised/tehnoloogilised lahendused (nt kaheastmeline autentimine) ajendavad küll inimesi küberturvalisemalt käituma, kuid siiski tingivad kohati küberhaavatavust nt ebaturvalised harjumused, hooletus, mugavus ja laiskus.</p> <p>Peamised riskikohad inimeste küberkäitumises on seejuures nt nõrkade paroolide kasutamine ning kaheastmelise autentimise vältimine.</p>	<p>Soosida selliste tehnoloogiliste lahenduse arendamist ja kasutamist, mis toetavad inimesi küberturvaliste praktikate rakendamisel, ent on samas ka kasutajasõbralikud. Nt eelistada eri veebilehtedel/rakendustes salasõnade asemel riigi autentimisteenuse (TARA) kasutamist, sisselogimise ajalõpu rakendamine jms. Koolitada ja toetada teenusepakkujaid era- ja avalikust sektorist pakkuma oma vaikimisi lahendusena just turvalisemaid võimalusi (nt vaikimisi sisselogimine TARA vahendusel, kasutajanime ja salasõna kasutamine teha keerulisemaks jne).</p> <p>Julgustada teenusepakkujaid (nt telekommunikatsiooniettevõtteid) jagama inimestele järjepidevalt küberturvalisusalast informatsiooni, et küberhügieeni järgimise olulisust inimestele järjepidavalt meelde tuletada. Telekommunikatsiooniettevõtted saavad nt koos paberarvetega saata inimestele teemakohaseid infovoldikuid (võiks olla eriti hinnatud lahendus eakate seas) või saavad juhendmaterjale jagada tehnikud kliendivisiidi korral.</p>

Kasutatud allikad

- Abbinante, A., Antonacci, A., Antonioni, M., Butera, A., Castaldi, M., Cotellessa, S., Di Marco, C., Gangale, M., Izzetti, R., Luperini, M., Maiorani, C., Nardi, G. M., Ravoni, A., Sabatini, S., Sestito, S., Virno, A., & Graziani, F. (2024). Concordance and clinical outcomes improvement following oral hygiene motivation: A systematic review and report of the workshop of the Italian Societies of Dental Hygiene. *International Journal of Dentistry*, Article ID 8592336, 1–12. <https://doi.org/10.1155/2024/8592336>
- Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: An approach for cyber security education training and awareness. *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden. AIS Electronic Library. https://aisel.aisnet.org/ecis2019_rp/100
- Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, 102258. <https://doi.org/10.1016/j.techsoc.2023.102258>
- Ajzen, I. (1991). *The theory of planned behavior*. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 13(9), 5700. <https://doi.org/10.3390/app13095700>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. ArXiv. <https://doi.org/10.48550/arXiv.1901.02672>
- Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, 142, 103858. <https://doi.org/10.1016/j.cose.2024.103858>
- Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A literature review. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity* (pp. 51–62). Springer. https://doi.org/10.1007/978-3-319-60585-2_25
- Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 52(2), 25–67. <https://doi.org/10.1145/3462766.3462770>
- Haridus- ja Teadusministeerium. (2021). *Haridusvaldkonna arengukava 2021–2035*. https://www.hm.ee/sites/default/files/documents/2022-09/1._haridusvaldkonna_arengukava_2035_kinnitatud_11.11.21.pdf

- Hedin, B., Katzeff, C., Eriksson, E., & Pargman, D. (2019). A systematic review of digital behaviour change interventions for more sustainable food consumption. *Sustainability*, *11*(9), 2638. <https://doi.org/10.3390/su11092638>
- Higgins, J. P. T., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M. J., & Welch, V. A. (Eds.). (2024). *Cochrane Handbook for Systematic Reviews of Interventions* (Version 6.5, updated August 2024). Cochrane. <https://www.training.cochrane.org/handbook>
- ITL. (s.d.). *Eesti CyberTech klaster*. <https://itl.ee/cybertech/>
- Kapukotuwa, S., Nerida, T. M., Batra, K., & Sharma, M. (2024). Utilization of the multi-theory model (MTM) of health behavior change to explain health behaviors: A systematic review. *Health Promotion Perspectives*, *14*(2), 121–135. <https://doi.org/10.34172/hpp.42887>
- Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security*, *149*, 104204. <https://doi.org/10.1016/j.cose.2024.104204>
- Kolodko, J., Schmidtke, K. A., Read, D., & Vlaev, I. (2021). #LetsUnlitterUK: A demonstration and evaluation of the Behavior Change Wheel methodology. *PLOS ONE*, *16*(11), e0259747. <https://doi.org/10.1371/journal.pone.0259747>
- Kwasnicka, D., Dombrowski, S. U., White, M., Sniehotta, F. (2016). Theoretical explanations for maintenance of behaviour change: a systematic review of behaviour theories. *Health Psychology Review*, *10*(3), 277–296. <https://doi.org/10.1080/17437199.2016.1151372>
- Küberturvalisuse seadus*. (2018). RT I, 22.05.2018, 1. <https://www.riigiteataja.ee/akt/121062024015>
- Majandus- ja Kommunikatsiooniministeerium. (2021). *Eesti digiühiskond 2030*. https://mkm.ee/sites/default/files/documents/2022-04/Digiühiskonnna%20ARENGUKAVA_13.12.2021.pdf
- Majandus- ja Kommunikatsiooniministeerium. (2024). *Küberturvalisuse strateegia 2024–2030. „Läbivald IT-vaatlikum Eesti“*. <https://www.mkm.ee/sites/default/files/documents/2024-12/Küberturvalisuse%20strateegia%202024-2030.pdf>
- Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, *6*(1), 42. <https://doi.org/10.1186/1748-5908-6-42>
- Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., Eccles, M. P., Cane, J., & Wood, C. E. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: building an international consensus for the reporting of behavior change interventions. *Annals of behavioral medicine : a publication of the Society of Behavioral Medicine*, *46*(1), 81–95. <https://doi.org/10.1007/s12160-013-9486-6>

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., and The PRISMA Group. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLOS Medicine* 6, e1000097. doi: 10.1371/journal.pmed.1000097

Murasov, M., Allemann, M., Preegel, K., Michelson, A. (2022). *Rahvaraamatukogude rolli analüüs ja ettepanekud valdkondadevahelise koostöö tõhustamiseks*. Tallinn: Poliitikauuringute Keskus Praxis. <https://vana.praxis.ee/wp-content/uploads/2022/01/Rahvaraamatukogude-rolli-analüüs.pdf>

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). Training and embedding cybersecurity guardians in older communities. In Y. Kitamura, A. Quigley, K. Isbister, T. Igarashi, P. Bjørn, & S. Drucker (Eds.), *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Article 86, pp. 1–15). Association for Computing Machinery. <https://doi.org/10.1145/3411764.3445078>

Peiris, C. L., Gallagher, A., Taylor, N. F., & McLean, S. (2023). Behavior change techniques improve adherence to physical activity recommendations for adults with metabolic syndrome: A systematic review. *Patient Preference and Adherence*, 17, 689–697. <https://doi.org/10.2147/PPA.S393174>

Politsei- ja Piirivalveamet. (2018). *Ennetustöö kontseptsioon*. <https://www.politsei.ee/files/Ennetus/politsei-ja-piirivalveameti-ennetust-kontseptsioon-sept-2018-.pdf?40da87a884>

Pollini, A., Callari, T. C., Tedeschi, A., & Galletta, A. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, 24(2), 371–390. <https://doi.org/10.1007/s10111-021-00683-y>

Prochaska, J. O., & Velicer, W. F. (1997). *The transtheoretical model of health behavior change*. *American Journal of Health Promotion*, 12(1), 38–48. <https://doi.org/10.4278/0890-1171-12.1.38>

Prümmer, J., van Steen, T., & van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>

Riigi Infosüsteemi Ameti põhimäärus. (2011). RT I, 28.04.2011, 1. <https://www.riigiteataja.ee/akt/127122024010>

Riigi Infosüsteemi Amet. (2023). *Küberturvalisuse aastaraamat 2023*. https://www.ria.ee/sites/default/files/documents/2023-02/RIA_kyberturvalisuse_aastaraamat_2023.pdf

Riigi Infosüsteemi Amet. (2025a). *Küberturvalisuse aastaraamat 2025*. <https://www.ria.ee/sites/default/files/documents/2025-02/RIA-kuberturvalisuse-aastaraamat-2025.pdf>

Riigi Infosüsteemi Amet. (2025b). *Küberturvalisuse keskuse põhimäärus*.

https://www.ria.ee/sites/default/files/vp_contacts/files/RIA-kuberturvalisuse-keskuse-pohimaarus-2025.pdf

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.

Salem, M. A., & Sobaih, A. E. E. (2023). A quadruple “E” approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in Saudi Arabia amid COVID-19 pandemic. *Electronics*, *12*(10), Article 2268.

<https://doi.org/10.3390/electronics12102268>

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection motivation theory in information security behavior research: Reconsidering the fundamentals.

Communications of the Association for Information Systems, *53*, 1136-1165.

<https://doi.org/10.17705/1CAIS.05348>

Trushna, T., Krishnan, K., Soni, R., Singh, S., Kalyanasundaram, M., Sidney Annerstedt, K., Pathak, A., Purohit, M., Stålsby Lundbog, C., Sabde, Y., Atkins, S., Sahoo, K. C., Roustia, K., & Diwan, V. (2024). Interventions to promote household waste segregation: A systematic review. *Heliyon*, *10*(2), Article e24332. <https://doi.org/10.1016/j.heliyon.2024.e24332>

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1), tyaa019. <https://doi.org/10.1093/cybsec/tyaa019>

Viru, K. (2025). *Eesti vanema täiskasvanu küberturvalise käitumise püsivuse toetamine*.

<https://hdl.handle.net/10062/111444>

Lisa 1. Meetodid ja andmed

Järgnevalt anname ülevaate uuringus kasutatud andmekogumis- ja analüüsimeetoditest.

Süstemaatiline kirjandusülevaade

Uuringu esimene etapp hõlmas süstemaatilise kirjandusülevaate koostamist ning inimeste (küber)käitumise püsivale muutmisele suunatud sekkumiste kaardistamist. Etapi eesmärk oli süstemaatiliselt kokku koondada parimad tõendus põhised sekkumised inimeste käitumise, sealhulgas küberkäitumise püsivaks mõjutamiseks ning seejärel neid sekkumisi ühistel alustel analüüsida.

Vastavalt uuringu tellija koostatud lähteülesandele käsitlesime ülevaates korraga nii üldisemaid käitumise mõjutamise mehhanisme ja sekkumisi, millel on tuvastatud püsiv mõju, kuid otsisime ka spetsiifiliselt küberkäitumise mõjutamisele keskendunud sekkumisi. See tähendab, et me ei piiritlenud ülevaatesse kaasatavat kirjandust huvipakkuva käitumise valdkonnaga, s.t kaasasime ülevaatesse sekkumisi lisaks küberturvalisele käitumisele ka teistest valdkondadest, nt tervise- või keskkonnakäitumise valdkondadest. Samuti ei piiritlenud me kaasatavat kirjandust kindla piirkonna ega riigiga.

Süstemaatilise ülevaate eesmärk oli vastata järgnevatele (alam)uurimisküsimustele:

- Milliseid käitumist püsivalt mõjutavaid sekkumisi on maailmas inimeste seas läbi viidud?
 - Millisele sihtrühmale ning mis eesmärgiga on sekkumised loodud?
 - Kes neid sekkumisi ellu on viinud ning kuidas (nt kuidas on tagatud ressursid)?
 - Millised neist sekkumistest on olnud kõige efektiivsemad, et inimeste käitumist püsivalt mõjutada? Kui mõju ei saavutatud, siis mis oli takistuseks?
 - Kuidas saaks neid sekkumisi rakendada küberkäitumise kontekstis?
- Milliseid tulemuslikke küberkäitumist püsivalt mõjutavaid sekkumisi on inimeste seas läbi viidud?
 - Millisele sihtrühmale ning mis eesmärgiga on sekkumised loodud?
 - Kes neid sekkumisi ellu on viinud ning kuidas (nt kuidas on tagatud ressursid)?
 - Mis on taganud nende sekkumiste tulemuslikkuse ehk mis on olnud n-ö edu tegurid?

Metoodika

Kasutasime tervisevaldkonna uuringute tarbeks välja töötatud süstemaatilise ülevaate meetodeid, järgides võimalikult täpselt PRISMA (Moher *et al.*, 2009) ja Cochrane Handbook for Systematic Reviews of Interventions (Higgins *et al.*, 2024) juhiseid, mille järgimine võimaldab

ka teistel uurijatel soovi korral protseduuri korrata. Just seetõttu kasutasime uuringute kaasamis- ja välistamiskriteeriumite määramisel ka PICOS-süsteemi.¹⁷

Süsteemaatilise ülevaate läbiviimine koosnes järgnevatest etappidest:

1. uurimisküsimuste täpsustamine;
2. kaasamiskriteeriumite määratlemine;
3. otsingustrateegia loomine;
4. uuringute pealkirjade ja lühikokkuvõtete skriinimine;
5. uuringute täistekstide skriinimine.

Esmalt teostasime süsteemaatilise ülevaate, kus prioriteet oli, et kaardistatavad käitumist mõjutavad sekkumised oleksid püsiva mõjuga. Allolevas tabelis (vt Tabel 2) toome välja selle ülevaate kaasamiskriteeriumid PICOS-süsteemi järgi. Kaasasime ülevaatesse ingliskeelsed uuringud, mis olid ilmunud viimase viie aasta jooksul (2021–2025, mõlemad k.a) ja mille täistekst oli vabalt kättesaadav.

Tabel 2. Esimese otsingu strateegia

PICOS element	Kriteerium	Otsingustrateegia
Probleem või populatsioon	alates 16-aastased inimesed	
Sekkumine	sekkumised käitumise ja hoiakute muutmiseks	(intervention* OR program* OR programme* OR training* OR campaign* OR educat* OR awareness) AND
Võrdlus	ükskõik milline kontrollgrupp	(„Long*term” OR longitudinal OR persist* OR sustain* OR retain*) AND
Tulemused	ükskõik millised tulemused, mis on seotud käitumise püsiva muutusega, kusjuures püsiv = vähemalt 6 kuud	(behavior OR behaviour OR "behavior change" OR "behaviour change" OR "behavior modification" OR "behaviour modification" OR "longitudinal behavior change" OR "longitudinal behaviour change" OR "habit formation" OR "attitude change" OR "cyber OR cybersecurity OR "cyber security" OR "digital security" OR "digital behaviour" OR "digital behavior" OR "secure behavior" OR "secure behaviour" OR "online security" OR "online security behavior" OR "online security behaviour" OR "internet safety" OR "internet safety behavior" OR "internet safety behaviour" OR "password manag*" OR "phishing" OR "phishing suscept*" OR "data protection" OR "data protection behavior" OR "data protection behaviour") AND
Kontekst või uuringutüüp	metaanalüüsid ja süsteemaatilised ülevaated	("meta*analysis" OR "systematic review" OR "systematic literature review")

¹⁷ PICOS-süsteemi elemendid: 1) probleem/populatsioon – *problem/population*, 2) sekkumine – *intervention*, 3) võrdlus – *comparison*, 4) tulemused – *outcomes*, 5) uuringu tüüp – *setting/study type*.

Me ei kaasanud ülevaatesse selliseid uuringuid, milles ei kogutud empiirilisi andmeid (nt arvamuskirjandus või pelgalt teoreetilised käsitlused); kus uuritav sekkumine ei olnud suunatud käitumise või hoiakute muutmisele, vaid kus tegemist oli hoopis tehnilist laadi sekkumisega küberturvalisuse parandamiseks. Samuti ei kaasanud me ülevaatesse selliseid uuringuid, kus sekkumise pikaajalist (vähemalt kuus kuud) mõju ei mõõdetud või kus mõju ei tuvastatud. Ka jäid ülevaatest välja uuringud, kus osalejateks olid vaid alla 16-aastased, ning sellised uuringud, kus käsitleti huvipakkuvat käitumist mõjutavaid tegureid (nt vanus või sotsiaaldemograafilised tunnused), kuid puudus sekkumine.

Süsteematisel kirjandusülevaate läbiviimisel selgus, et ükski küberturvalise käitumise sekkumist käsitletud uuring ei vastanud seatud kriteeriumitele ning seepärast otsustasime viia läbi ka teise, väiksema mahuga ning täpsustatud otsingu, kus fookus oli just küberturvalise käitumise sekkumistel ning kuhu kaasasime ka üksikuuringuid, mitte vaid ülevaateuuringuid. Selle otsingu kaasamiskriteeriumid on toodud välja allolevas tabelis (vt Tabel 3).

Tabel 3. Teise otsingu strateegia

PICOS element	Kriteerium	Otsingustrateegia
Probleem või populatsioon	alates 16-aastased inimesed	(intervention* OR program* OR programme* OR training* OR campaign* OR educat* OR awareness)
Sekkumine	sekkumised küberturvalise käitumise või sellega seotud hoiakute muutmiseks	AND (cyber OR cybersecurity OR "cyber security" OR „digital security" OR „digital behaviour" OR „digital behavior" OR „secure behavior" OR „secure behaviour" OR „online security" OR „online security behavior" OR „online security behaviour" OR „internet safety" OR „internet safety behavior" OR „internet safety behaviour" OR „password manag*" OR phishing OR „phishing suscept*" OR „data protection" OR „data protection behavior" OR „data protection behaviour") AND (behaviour OR behavior)
Võrdlus	ükskõik milline võrdlus (sh kontrollgrupp, enne-pärast testid)	
Tulemused	ükskõik millised tulemused, mis on seotud küberturvalise käitumise püsiva muutusega, kusjuures püsiv = vähemalt 6 kuud	(„Long*term" OR longitudinal OR persist* OR sustain* OR retain*)
Kontekst või uuringutüüp	empiirilised uuringud (mitte arvamuskirjandus, uuringuprotokollid või vaid teoreetilised käsitlused)	

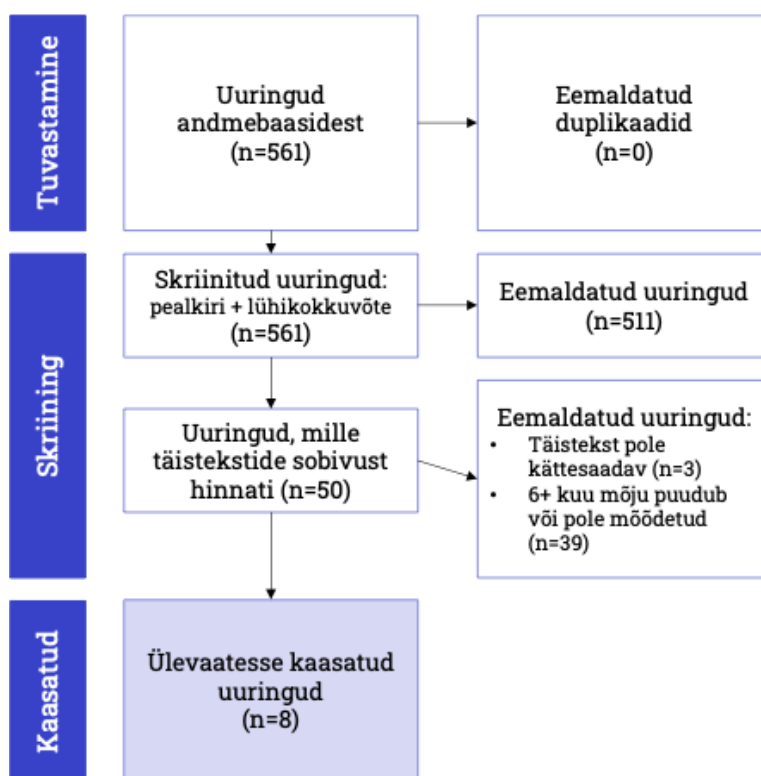
Ka teises ülevaates kaasasime otsingusse viimasel viiel aastal (2021–2025, mõlemad k.a) ilmunud ingliskeelsed artiklid, mille täistekst oli vabalt kättesaadav.

Mõlemad otsingud viisime läbi Web of Science andmebaasi kasutades.

Tulemused

Esimene otsing

Tuvastasime andmebaasist 9. mai 2025 seisuga 561 meie kaasamiskriteeriumitele vastavat artiklit ning kasutasime otsingus tuvastatud uuringute skriinimiseks Covidence'i keskkonda. Joonis 3 annab ülevaate leitud uuringute skriinimise protsessist. Pealkirja ja lühikokkuvõtte skriiningu tulemusel jäid valimist välja 511 artiklit. Peamine väljajätmise põhjus oli püsiva mõju (või selle mõõtmise) puudumine uuringutes, mida leitud artiklid käsitlesid. Seega jäi pealkirja ja lühikokkuvõtete skriiningu järel sõelale 50 uuringut, mille ülevaatamise järel eemaldasime valimist veel kolm uuringut, mille täistekst polnud kättesaadav ning 39 uuringut, kus sekkumise püsivat mõju ei tuvastatud või ei mõõdetud. Seega kaasasime täistekstide ülevaate tulemusel oma analüüsi lõpuks kaheksa uuringut, mis vastasid kõigile kriteeriumitele. Ülevaatesse kaasatud uuringutes käsitleti käitumise muutmiseks loodud sekkumiste mõju väga erinevates valdkondades (nt tervisekäitumine, tarbimiskäitumine, vanemlus).



Joonis 3. Süstemaatilise ülevaate PRISMA-skeem. Allikas: autorite koostatud

Teine otsing

Teise otsingu viisime läbi 21. aprillil 2025 ning selle tulemusena tuvastasime 110 artiklit, mida samuti Covidence'i kasutades kahes etapis (pealkirjad ja lühikokkuvõtted ning seejärel täistekst) skriinisime. Mitte ühegi kõigile teistele kriteeriumitele vastanud sekkumise puhul polnud mõõdetud või tõendatud sekkumise pikaajaline soovitud mõju käitumisele. Ka teised

uurijad on sekkumiste pikaajalise mõju ja selle mõõtmise puudumist küberturvalisuse edendamise kitsaskohana välja toonud (Prümmer *et al.*, 2023) ning seega osutab see laiemale probleemile küberturvalise käitumise uurimises ja edendamises.

Konsulterides uuringu tellijaga, otsustasime teise, küberturvalisusalastele sekkumistele keskendunud otsingu tulemustest siiski kaks paljulubavat sekkumist hõlmata sekkumiste rakendatavuse hindamisse vaatamata sellele, et nende puhul polnud tõendatud või mõõdetud sekkumise pikaajalist mõju käitumisele.

Sekkumiste võrdlemine ja nende rakendatavuse hindamine

Sekkumisi, mis süstemaatilise kirjandusülevaate teostamise järel sõelale jäid, kirjeldasime järgmiste näitajate abil: sihtrühm, valdkond, sekkumise sisu, käitumise muutus, peamine käitumise muutmise tehnika, püsiv mõju, hinnangud rakendatavusele¹⁸.

Sekkumistes kasutatud käitumise muutmise tehnikad määrasime vastavalt Michie *et al.* (2013) käitumise muutmise tehnikate taksonoomiale.

Selleks, et hinnata uuringusse kaasatud sekkumiste rakendatavust, hindas neid esmalt sõltumatu küberturvalisuse ekspert, kes keskendus eeskätt sellele, kuivõrd vastab sekkumine küberturvalisuskäitumise probleemidele Eestis ning mil määral on sekkumine Eesti kontekstis rakendatav. Pärast küberturvalisuse eksperdi hinnanguid otsustasime rakendatavuse hindamisega edasi minna nelja sekkumisega kaheksast esimese otsingu tulemusena ülevaatesse kaasatud sekkumisest ning kahe sekkumisega teisest, küberturvalisusalastele sekkumistele keskenduva otsingu tulemustest. Ülejäänud sekkumiste korralduse, sihtrühmade spetsiifilisuse või sekkumise sisu tõttu ei hinnanud sõltumatu ekspert neid küberturvalise käitumise ja RIA kontekstis piisavalt asjakohaseks või kohandatavaks.

Pärast sõltumatu eksperdi hinnangute saamist, korraldasime virtuaalse arutelukohtumise kahe RIA esindajaga. Arutelukohtumisel tutvustasime neile sõelale jäänud sekkumisi ja lasime neil sekkumiste rakendatavust hinnata arutelul, kus keskendusime järgmistele küsimustele:

- Kuidas seda tehnikat RIA praktikas kasutada (nt kampaania, koolitus, muu formaat)?
- Milliste sihtrühmade küberturvalisuse parandamiseks see sobiks?
- Milliseid takistusi või riske tuleb sellise sekkumise rakendamise juures silmas pidada?
- Milliseid ressursse on sekkumise rakendamiseks vaja?
- Kui vastuvõetav ja tõhus see sekkumine teie kogemuse ja tunnetuse põhjal sihtrühma(de)le oleks?

¹⁸ Hinnang rakendatavusele põhineb kolme küberturvalisuse valdkonna eksperdi (üks sõltumatu ekspert ning kaks tellija ehk RIA esindajat) arvamusel.

Sekkumistest, mis süstemaatilise kirjandusülevaate tulemusena sõelale jäid, oleme ülevaate andnud peatükis 4.

Intervjuud

Tegime uuringu käigus nii eksperdiintervjuusid kui fookusrühma- ja individuaalintervjuusid Eesti elanikega erinevates vanuserühmades. Järgnevalt toome välja täpsema ülevaate kõikidest tehtud intervjuudest, nende valimist ja intervjuude läbiviimise korraldusest. Detailse ülevaatega tehtud intervjuudest saab tutvuda ka alltoodud tabelis (vt Tabel 4).

Ekspertiintervjuud

Esmalt teostasime eksperdiintervjuu RIA esindajaga, et saada lisainfot uuringu tausta ja Eesti inimeste küberkäitumisega seotud trendide kohta ning täiendada ülevaadet küberturvalisusealase ennetus- ja teavitustöö korralduse ning seni elluviidu (sh varasemate RIA teavitus- ja ennetustegevuste) osas.

Lisaks RIA esindajale intervjuerisime veel nelja Eesti eksperti, kes oma igapäevatöös on seotud küberturvalisuse alase teavitus- ja ennetustööga, kas selle uurimise või praktilise korraldamise mõttes. Nende eksperdiintervjuude eesmärk oli saada täiendavat infot seni tehtud teavitus- ja ennetustöö kohta ning ühtlasi kuulda, millised on olnud ekspertide õppetunnid ja tähelepanekud seda tööd tehes.

Kasutades sihiteadlikku valimit (lähtudes sh ka tellija soovitudest), intervjuerisime:

- PPA esindajat;
- Pangaliidu esindajat;
- ITL-i esindajat;
- küberturvalisuse eksperti.

Kõikide eksperdiintervjuude läbiviimiseks koostasime poolstruktureeritud intervjuukavad, mille küsimused olid kohandatud lähtuvalt konkreetse intervjueritava profiilist. Kõik eksperdiintervjuud toimusid individuaalintervjuudena videokõne rakenduse Microsoft Teams abil. Ühe intervjuu kestus oli kuni 50 minutit.

Fookusrühma- ja individuaalintervjuud Eesti elanikega

Lisaks eksperdiintervjuudele tegime uuringu käigus intervjuusid Eesti elanikega kolmest eri vanuserühmast (16–24, 35–44 ja 55–64-aastased¹⁹). Nende intervjuude eesmärk oli uurida inimeste küberturvalisuse käitumist: nt seda, milliseid häid kogemusi või õppetunde neil küberturvalisusega seoses on; mis põhjusel inimesed rakendavad või ei rakenda

¹⁹ Nimetatud vanuserühmad kuulusid uuringu valimisse vastavalt uuringu tellija soovile.

küberturvalisuse parimaid praktikaid ja kuidas saaks Eesti elanike küberturvalist käitumist nende endi arvates tõhusamalt toetada.

Kokku intervjueerisime uuringu käigus 46 inimest. Järgnevalt toome vanusegrupiti välja intervjueeritud inimeste arvu ja tausta ning tehtud intervjuude formaadid:

- 16–24-aastased Eesti elanikud – kokku 19 intervjueeritavat
 - Viisime läbi kaks fookusrühma intervjuud (kummaski neli osalejat) ja 11 individuaalset telefoniintervjuud.
 - Intervjueeritavatest enamus (15) olid naissoost. Enim oli intervjuul osalejaid Tartumaalt (10) ja Harjumaalt (7). Lisaks oli üks intervjueeritav Võrumaalt ning üks Ida-Virumaalt.
- 35–44-aastased Eesti elanikud – kokku 15 intervjueeritavat
 - Viisime läbi kaks fookusrühma intervjuud (ühes kolm ja teises neli osalejat) ja 8 individuaalset telefoniintervjuud.
 - 10 intervjueeritavat olid nais- ja 5 meessoost. Maakondade lõikes oli enim intervjueeritavaid Harjumaalt (11). Esindatud olid ka Tartumaa (3) ja Lääne-Virumaa (1).
- 55–64-aastased Eesti elanikud – kokku 12 intervjueeritavat
 - Vanima vanusegrupi esindajatega teostasime individuaalsed telefoniintervjuud.
 - Intervjueeritavatest 10 olid nais- ja 2 meessoost. Enim oli intervjuul osalejaid Harjumaalt (4). Ida-Virumaalt, Võrumaalt, Tartumaalt ja Hiiumaalt osales igäühel intervjuul kaks inimest.

Intervjueeritavate värbamiseks kasutasime mitut eri lähenemist. Keskmise ja vanima vanusegrupi esindajate leidmiseks kontakteerusime esmalt eri piirkondade maakonna- või linnaraamatukogudega (kokku 18 erinevat raamatukogu²⁰), kel palusime osalemiskutset levitada oma sotsiaalmeedia jt infokanalite vahendusel. 16–24-aastaste intervjueeritavate värbamiseks võtsime aga meili teel ühendust Tartu Ülikooli, Tallinna Ülikooli ja Tallinna Tehnikaülikooli üliõpilasesindustega ning kutseõppeasutuste ja gümnaasiumide õpilasesindustega Kesk-, Kirde-, Lõuna-, Lääne- ja Põhja-Eestist²¹ (kokku kuulus kontakteerumislisti üheksa kutseõppeasutust ja 10 gümnaasiumit) ning palusime neil olla abiks osalemiskutse jagamisel oma õppeasutuste õppurite seas.

Kuna mainitud viisidel ei õnnestunud koguda piisaval hulgal intervjueeritavaid, postitasime lisaks intervjuudel osalemise kutse korduvalt Praxise sotsiaalmeediakanalitesse (Facebook ja Instagram). Ühel korral levitas infot intervjuude toimumise kohta ka RIA oma Facebooki kontol. Ühtlasi rakendasime lumepallivalimit ja palusime juba intervjuudel osalenutel levitada infot meie uuringu toimumise kohta ning kontakteerusime ka otse inimestega oma suhtlusringkonnas, kes valimi kriteeriumitele vastasid. Motiveerimaks inimesi intervjuul osalema, premeerisime kõiki intervjuul osalejaid 15-euroste e-kinkekaartidega. Kõikide

²⁰ Lähtusime Kultuuriministeeriumi maakonnaraamatukogude ja suuremate linnade keskraamatukogude loendist. Vt lähemalt [Kultuuriministeeriumi veebilehelt](#).

²¹ Lähtusime NUTS III taseme jaotusest.

alaealiste intervjuueeritavate puhul palusime ühtlasi nende seaduslikult esindajalt allkirjastatud nõusolekut, et noor võiks intervjuul osaleda.

Kõik fookusrühma intervjuud korraldasime videokõne teel rakenduse Microsoft Teams abil ja need kestsid ligikaudu 60 kuni 105 minutit. Individuaalintervjuud telefoni teel kestsid kuni 30 minutit. Nii fookusrühma- kui individuaalintervjuude teemad panime paika lähtudes uurimisküsimustest. Intervjuu kava oli ühesugune, olenemata intervjuu formaadist.

Tabel 4. Ülevaade uuringu käigus teostatud intervjuude sihtrühmadest, valimist ja formaadist

Sihtrühm	Intervjuude arv / intervjuul osalejate koguarv	Formaat
Eksperdid	5 / 5	Individuaalintervjuu videokõne vahendusel
16–24-aastased Eesti elanikud	2 + 11 / 19	2 fookusrühmaintervjuud videokõne vahendusel + 11 individuaalintervjuud telefoni teel
35–44-aastased Eesti elanikud	2 + 8 / 15	2 fookusrühmaintervjuud videokõne vahendusel + 8 individuaalintervjuud telefoni teel
55–64-aastased Eesti elanikud	12 / 12	Individuaalintervjuud telefoni teel

Intervjuude analüüs

Osalejate nõusolekul salvestasime kõik intervjuud ja transkribeerisime salvestused, et kasutada kogutud teavet analüüsis. Andmeanalüüsimeetodina kasutasime nii eksperdi- kui Eesti elanikega teostatud intervjuude puhul kvalitatiivset kontentanalüüsi, mis sobib mõõduka suurusega valimiga ning meie eesmärgiga uurida eri osapoolte kogemusi seoses küberturvalise käitumise edendamise (ekspertide puhul); inimeste käitumismustreid ja motivaatoreid, õppetunde, toe- ning infovajadust jne. Intervjuude käigus kogutud materjali süstematiseerisime ja analüüsisime eelnevalt paika pandud teemade kaupa (nt küberturvalisusealase ennetus- ja teavitustöö korraldus, küberturvalise käitumise praktikad, motivaatorid, infovajadus, õppetunnid, teavituskanalid jms).

Järelduste ja soovitude sõnastamine

Uuringu järeldused ja soovitused tuginevad nii süstemaatilise kirjandusülevaate kui ka intervjuude käigus kogutud andmete analüüsile.

Järelduste ja soovitude koostamisse on sisendi andnud kogu uurimismeeskond, sh uuringusse kaasatud küberturvalisuse ekspert Liisa Past, lähtudes põhimõttest, et kõik järeldused peavad tulenema konkreetsetest analüüsileidudest ning kõik soovitused peavad olema seotud vähemalt ühe järeldusega.