TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Kati Sein 204777IVCM

CYBERSECURITY-RELATED SUPPORT NEEDS AND CHALLENGES INCURRED BY INFORMAL SUPPORT: A STUDY AMONG ESTONIAN HOME USERS

Master's Thesis

Supervisor: Stefan Sütterlin
PhD

Co-supervisor: Tanel Mällo
PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kati Sein 204777IVCM

VAJADUSED KÜBERTURVALISUSEALASE TOE JÄRELE JA MITTEAMETLIKU TOEGA KAASNEVAD VÄLJAKUTSED: UURING EESTI TAVAKASUTAJATE SEAS

Magistritöö

Juhendaja: Stefan Sütterlin
PhD

Kaasjuhendaja: Tanel Mällo
PhD

Tallinn 2024

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kati Sein

11.05.2024

Abstract

Estonia offers citizens a wide range of e-services [1] and is a prominent "cybersecure" country according to the Global Cybersecurity Index [2]. Nevertheless, there is no single dedicated cybersecurity support service to assist laypeople with diagnosing and solving cybersecurity issues in private matters. Instead, their friends and family seem to serve as the first line of assistance. The aim of this study is to unveil Estonian home users' needs for cybersecurity-related assistance. The study employs the concept of tech caregiving, where individuals voluntarily assist each other, narrowing it to the cybersecurity field and coining a term *cybersecurity caregiving*. It asks in which cybersecurity-related situations laypeople would ask for external help, what characterises the cybersecurity support they seek, and how different the expectations are from what they currently receive from their cybersecurity caregivers. The research also examines challenges incurred by the current informal support by investigating unsecure practices occurring during informal support sessions.

Exploratory sequential mixed methods approach was chosen to address the research problem. Seven interviews with cybersecurity caregivers were conducted and analysed thematically, informing the development of a survey questionnaire targeting the adult population of Estonia. The statistical analysis of the survey results (n=161) revealed that cyber situational awareness and incident handling questions would induce the majority of participants to seek help. The respondents valued accuracy, speed, accessibility, understandability and cost as important characteristics of cybersecurity support in private matters. These qualities also described the current informal support they received from their cybersecurity caregivers, only it could be received more quickly. Also, the majority of respondents assessed the current support from cybersecurity caregivers as sufficient. Some respondents admitted engaging in unsecure practices like granting their helper full control over their device, developing dependence on them, or disclosing credentials or sensitive information. Middle-aged male participants with higher education and employed with jobs involving extensive Internet usage more often than other groups reported knowledge of a solution to a particular cybersecurity issue. Other groups like the unemployed, students or the retired could be considered less prepared for securely acting in cyberspace. Most respondents demonstrated a willingness to seek help if they were unable to find a solution themselves, rather than leaving the issue unaddressed.

Although many Estonian home users report that their current informal support is sufficient, these findings encourage a conclusion that the society would benefit from dedicated cybersecurity support to assist laypeople with cybersecurity issues in their private matters. Also, by empowering the cybersecurity caregivers with resources tailored to them and teaching laypeople to declare their cybersecurity requirements and minimise unsecure practices, the cybersecurity caregivers could be valuable allies to the state in improving the overall cybersecurity posture of the population. By extending our understanding of the home users' needs for cybersecurity-related support and the negative sides of cybersecurity caregiving, this study provides the bases for policy making to enhance the population's cyber resilience.

The thesis is written in English and is 78 pages long, including 8 chapters, 7 figures and 12 tables.

Annotatsioon

Vajadused küberturvalisusealase toe järele ja mitteametliku toega kaasnevad väljakutsed: uuring Eesti tavakasutajate seas

Kuigi Eesti pakub kodanikele laia valikut e-teenuseid [1] ja on sealjuures globaalse küberturvalisuse indeksi [2] järgi silmapaistvalt "küberturvaline" riik, puudub siin tugiteenus, mille poole eraisik võiks igasuguse küberturvalisuse alase küsimuse korral pöörduda. Paljudel juhtudel täidab sellise esmatasandi toe rolli vabatahtlikult inimese sõber või sugulane. Käesoleva lõputöö eesmärk on selgitada välja Eesti tavakasutajate vajadused küberturvalisuse alase toe järele. Selles uuritakse, millistes küberturvalisusega seotud olukordades nad nõu küsiksid, mis on küberturvalisusealase abi juures oluline ja kas praegu saadav mitteformaalne tugi vastab neile ootustele. Kirjeldatakse ka ebaturvalisi teguviise, mis eraisikute omavahelise abistamisega kaasneda võivad.

Uurimisprobleemile läheneti eksploratiivselt ja rakendades kombineeritud uuringudisaine järjestikuliselt. Viidi läbi seitse intervjuud inimestega, kes oma sõpru või sugulasi küberturvalisuse alastes küsimustes aitavad. Intervjuude temaatiline analüüs andis teavet Eesti täiskasvanud elanikkonnale suunatud küsimustiku väljatöötamiseks. Veebiküsitluse tulemuste (n=161) statistiline analüüs näitas, et kõige enam tuntakse vajadust abi järele olukorrateadlikkuse ja intsidendihalduse küsimustes. Eraelus saadava küberturvalisuse alase abi juures peeti oluliseks selle täpsust, kiiret kättesaadavust, lihtsust selle küsimisel, selgituste arusaadavust ning et see oleks tasuta. Samad omadused kirjeldasid ka praegu oma sõbralt või sugulaselt saadavat abi, ainult see võiks olla kiiremini kättesaadav. Enamik neist, kel isiklik küberturvalisuse abistaja olemas, pidasid saadavat abi piisavaks. Mõned vastajad tunnistasid, et on andnud abilisele täieliku kontrolli oma seadme üle, muutunud temast sõltuvaks või avaldanud talle oma konto pääsumandaate. Kõrgharidusega keskealised meessoost vastajad, kes tööalaselt kasutavad palju internetti, märkisid teistest sagedamini, et nad teavad lahendust küsitavale küberturvalisusealasele probleemile. Teised elanikkonna rühmad (töötud, üliõpilased, pensionärid, internetikasutusega vähe seotud ametites töötavad) on iseseisvalt ja turvaliselt küberruumis tegutsemiseks vähem valmis. Probleemi ignoreerimise asemel ilmutas enamik vastanutest valmisolekut otsida abi, kui ei suuda ise lahendust leida.

Seega kuigi paljude tavakasutajate arvates on praegune teiselt eraisikult saadav küberturvalisuse alane abi neile piisav, ei ole see siiski kõigile kättesaadav. Nii järeldab antud töö, et Eestis oleks vaja kõigile ligipääsetavat küberturvalisuse alast tugiteenust. Siinjuures isikud, kes teisi vabatahtlikult küberturvalisuse küsimustes juba aitavad, võivad osutuda riigile elanikkonna küberturvalisuse olukorra parandamisel väärtuslikeks partneriteks. Igal juhul tuleb tavakasutajaid õpetada sõnastama isiklikke nõudeid küberturvalisusele ja end abi küsides nii vähe kui võimalik haavatavasse olukorda seadma. Laiendades olemasolevaid teadmisi tavakasutajate küberturvalisuse alastest vajadustest ja mitteformaalse toe negatiivsetest külgedest, pakub käesolev uurimus poliitikakujundajatele teavet, millest lähtuda elanikkonna küberkerksuse tõstmisel.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 78 leheküljel, 8 peatükki, 7 joonist, 12 tabelit.

List of Abbreviations and Terms

ANOVA	analysis of variance
CERT-EE	Cyber Emergency Response Team of Estonia
CIA triad	security properties of confidentiality, integrity, availability
DESI	Digital Economy and Society Index
DDoS attack	distributed denial-of-service attack
DNS	Domain Name System
DSL modem	digital subscriber line modem
FAQ	frequently asked questions
GDPR	General Data Protection Regulation
IP	Internet Protocol
IoT	Internet of things
IT	information technology
MFA	multi-factor authentication
NCSC-EE	National Cyber Security Centre of Estonia
PIN	personal identification number
RIA	Estonian State Information Authority (Riigi Infosüsteemi Amet)
SEM	standard error of mean

Table of Contents

List of Figures

List of Tables

1. Introduction

In Estonia, not all citizen segments have access to cybersecurity-related assistance and support that would be competent, trustworthy, free of charge and would respond in a timely manner. When facing a cybersecurity issue, laymen turn to their social circles instead of consulting a dedicated and knowledgeable support service – as did the friends of the author asking the following questions.

"What should I do when my device shows a control code different from the one in the web browser? I was trying to log in to an e-service portal that handles really sensitive information. Who is hacked – my device, the portal I am logging into or the authentication provider? Should I inform them? Or... whom should I inform?"

"Somebody I know suggested a link. I know I should not click on suspicious links. How can I decide – is this link suspicious, or am I simply overreacting?"

"I received a phishing mail that looks very plausible. I want to report it so other people would be warned about it. Where should I forward it?"

"I was an organiser of an international online course, and now my partners abroad wish to add the image of my handwritten signature to the course certificate to be issued to the participants. I do not feel sharing a photo of my signature is okay. Is there a guideline recommending how to act in such a situation?"

These questions demonstrate that Estonian laypeople do not always know how to decide on a safe action. Although maybe trivial to a cybersecurity expert, these questions deserve proficient answers. What are the possibilities for citizens to get answers to cyber-related questions, apart from googling and asking ChatGPT, their relatives or friends?

According to the public narrative, Estonia and Estonians are outstanding in several aspects. First, Estonia is *the world's most advanced digital society* [3], *the digital republic* [4], a *digital miracle* [5], while Estonians are the *digital nation* [6] and a *tech-savvy nation* [7]. This image does not originate (solely) in public lore, rather these phrases derive from the official Estonian branding website managed by Estonian Business and Innovation Agency [8]. Second, backed by the fact that in 2020, Estonia ranked as the 3rd most secure country on the Global Cybersecurity Index [2], Estonia is proud of having the reputation as an

international cybersecurity leader [9], [10]. Third, as indicated by the DESI 2022 index [1], Estonia stands out for a very high number of e-government services addressed to and adopted by its citizens. Several of these e-services are seldom seen in other countries: usage of qualified electronic signatures in day-to-day administrative affairs, internet voting, applying for subsidies, applying for kindergarten, reporting on catch of fish [11]. The author asks: is every citizen able to behave in cyberspace in a secure and privacy-preserving way and diagnose cybersecurity issues on their own?

People who are poorly prepared to operate in cyberspace can pose a risk to themselves, their social circles, and the whole society.[1] The amount of connected devices under their administration is large, ranging from mobile phones, tablets, smart home devices, wearables, and home routers to IP cameras. These devices contain large amounts of private data that have to be curated wisely. Individuals are responsible for securing the vast number of accounts they have created during their online activities. At the disposal of criminals, these devices, accounts and data become tools, exploitation of which has the potential to harm not only individuals but the society at large. Data about users and their social networks helps tailor phishing or spear-phishing campaigns and recruit insiders for cyber espionage. Hijacked social media accounts provide criminals with a highly valuable platform for executing their campaign towards the list of contacts who trust the owner of the stolen account. Accounts related to e-commerce activities give access to payment options. Home routers, IP cameras, and IoT devices are easily exploited since they are exposed to the Internet and often deployed with default configurations and weak or hard-coded passwords. For example, in 2011, the Brazil society experienced a mass attack when, among other devices, compromised home DSL modems were configured to direct victims to fake pages of banks or install malware [13]. Famous cases of successful DDoS attacks using botnets of compromised home devices include the taking down of Microsoft Xbox Live and Sony Playstation Networks [14], the "achievements" of the Mirai malware [15], [16], and the attack against the DNS provider Dyn [17]. Last but not least, cybersecurity of laypeople matters because their lives become more and more dependent on technology. This reliance is increased by themselves (like by installing smart refrigerators, using activity trackers, health tech) [18, p. 44] but also by state agencies and other organisations who process their personal data.

For a citizen, communication with the state directly impacts their and their family's well-being. For a citizen of Estonia, it also involves creating, exchanging and storing sensitive private information in digital form. Therefore, this communication has to be completed "cyber securely" at both ends: on the authorities' side and the citizen's. Supposedly, the

[1] For an overview of how criminals can benefit from home users' devices and accounts and how it may affect the individual or the society, see the poster published by the SANS institute [12].

employees of Estonian government agencies are educated and backed by professional cybersecurity support to fulfil their duty. On the contrary, the citizens are to manage without one dedicated support service, yet it is their data and welfare that is at stake. The European Union cybersecurity Strategy for the Digital Decade clearly states that "EVERYONE should be able to safely live their digital lives" [19] and one way to achieve that is through deterring and responding to cyber threats with civilian and disaster response [20, pp. 13-14]. As the former Chief Information Officer Luukas Ilves put it, successful are societies that quickly implement new technologies but also make the effort to aid the whole society to adapt [21]. The current research aims to explore the needs for and reality of cybersecurity-related support among Estonian citizens.

One aspect of cyber hygiene is knowing where to find dedicated expert help in case of need. There are helplines for individual e-services (like chat box at id.ee for issues with logging in using Estonian ID-card, or "Write to help@ria.ee" at eesti.ee) and cyber hygiene awareness campaigns websites like Ole valmis! [22] and Be IT-conscious [23]. However, preliminary knowledge about the name of the service or web address of the site is a prerequisite to find these. One can turn to the police when something bad has already happened, e.g., an incident, and the victim has experienced consequences [24]. The CERT-EE gathers information about malicious activities also encountered by the citizens, but their ability to assist laypeople in real-time cyber incident handling is limited. Their priority is to provide cybersecurity support for the public sector institutions and the vital service providers. People who work for an employer who takes cybersecurity seriously may benefit from the training provided at work. Also, IT personnel of their employer could help solve cybersecurity incidents in their private lives, but their willingness depends on whether the employer's policies allow this. Individual 24/7 cybersecurity hotlines are offered by the private sector [25]. Being designed for securing the privacy and cybersecurity of key personnel of organisations, it is likely not accessible nor affordable for most citizens.

The author observes that laypeople in Estonia are not supported by one dedicated service to assist them in using e-government services or personal devices in a secure and privacy-preserving manner. By this they mean a synchronous or near-synchronous channel for assisting individuals with the initial diagnosis of the cybersecurity issue – like the family doctor's hotline established in Estonia [26], [27]. Currently, the task of analysing and solving their cybersecurity-related issues seems to be carried out by their immediate peers – a friend or a family member. This situation has its pros and cons. Strengthening social relationships, self-perceived expertise and uneven access to such peers can cause deficient and unequal preparedness for digital security and privacy management among the population. If a community has no access to a security or IT expert, a member who has demonstrated confidence with computers is asked to solve the issue. It can happen

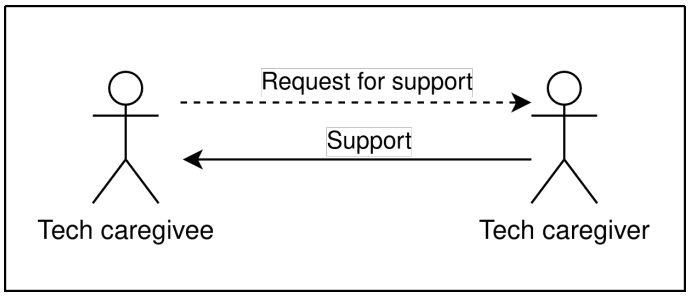

Figure 1. Tech caregiving as a relationship. Tech caregiver offers support (unbroken arrow) to tech caregivee reactively upon their request (dotted arrow) or proactively without it. In the current work, the term cybersecurity caregiving will be used analogously to tech caregiving.

that a juvenile who types quickly on the keyboard and googles fast is asked to help in everything that concerns the Internet or devices, including cybersecurity problems. They might solve the issue (the business process can continue), but their lack of expertise can open up another vulnerability. Also, the availability of a friend or relative is not always guaranteed, which postpones the solution or may even cancel it. Should people lack the ability to find existing service-specific support or differentiate suspicious situations from neutral ones on time, they are exposed to potential financial, physical or emotional harm.

1.1 On Terminology and Concepts

In the following, the term *home user* refers to an information technology user in home context where access to cybersecurity support is not provided officially. By official or institutional support, the author considers means pre-known to the user: support organised by their employee, university, a public or private service. The term *home user* is widely used in relevant academic literature [28], [29], [30], [31] as an antonym for *organizational user* or *employee*. The emphasis is on the situation or context where official help is not established. As such, the term refers to children and grown-ups equally. Other terms used in literature and carrying the same meaning include *citizen* [32], *individual* [33], *layman/laypeople*, and *private person*.

Cybersecurity caregiving is a concept to describe the phenomenon of individuals assisting each other in cybersecurity and digital privacy issues. The term is built upon and will be used analogously to an existing term *technology caregiving*. In the literature, technology or *tech caregiving* describes situations where individuals offer informal support and advice about technology to people they care about without necessarily being trained for this role nor receiving any reward in return [34], [35]. Tech caregiving involves support and advice on any technology, not only in the field of cybersecurity and digital privacy. One reason for this inclusion is that informal assistance in cybersecurity issues usually happens in more

general information technology support, e.g. troubleshooting issues or setting up a new device [34]. The other reason could be that cybersecurity caregiving as a newer conception has not been under the researchers' focus for a sufficient duration to facilitate the emergence and establishment of specific terms. Cybersecurity caregiving as a relationship has two parties: *cybersecurity caregiver* and *cybersecurity caregivee*. Cybersecurity caregivee is the party who reaches out for help or seeks information from the cybersecurity caregiver. Cybersecurity caregiver is the one who assists in solving issues and answers questions in the course of caregiving session (Figure 1).

The author acknowledges that the terms caregiver and caregivee may imply an unequal relationship, with the caregivee being perceived as a passive recipient and the caregiver as an active provider. It is important to recognise that this dynamic is not always the case. The cybersecurity caregivee may possess knowledge or expertise in another cybersecurity or privacy question and the cybersecurity caregiver can also learn in the advising process. Depending on the situation, their roles may even interchange. This choice of terms is obviously a simplification that is done to facilitate the discussion.

1.2 Research Questions

To explore the need for cybersecurity-related support among Estonians, initial research questions aimed at understanding the requirements for and experience with first-level cybersecurity assistance were formulated. In the course of the study (as described further in Sections 3.1 and 4), the initial questions were revised for relevance. This iterative process allowed grounding the research on the most current understanding of the situation faced by home users in Estonia and meet the expectations of the government policymakers. Specifically, consulting with the leading experts of the National Cyber Security Centre (now NCSC-EE) [36] informed the author how to contribute to intervention planning. They urged to know what are the cybersecurity topics or domains where citizens feel the biggest need for support, and how these needs vary among different population segments. Also, literature calling for research aiming at understanding the risks that coexist with relying largely on informal support [28], [37] was found. The final research questions are presented as follows.

RQ1: In which cybersecurity-related situations Estonian home users would ask for external advice or assistance?

RQ2: What characterises the cybersecurity support that Estonian home users seek?

RQ3: How different is the cybersecurity support Estonian home users receive from their

friends or family from the support they seek?

RQ4: What problems characterise the informal cybersecurity support that Estonian home users receive?

RQ5: How do answers to the preceding questions depend on sociodemographic variables or Internet usage?

1.3 Novelty, Scope and Goal

Cybersecurity behaviour of employees in organisations of all sizes is a field well covered by research utilising a wide range of qualitative as well as quantitative methods [38]. The literature shows that the effects of and response to different support, preventive and intervention mechanisms are often described and analysed in organisational contexts. On the contrary, the cyber incident management capabilities and support needs of individuals outside of work contexts are fields where thorough research is scarce.

By exploring the needs for and reality of cybersecurity-related support among Estonian citizens, this research aims to add to an informed foundation for intervention planning. This study will advance the understanding of the cybersecurity posture of Estonian home users by exploring it through the prism of cybersecurity caregiving. Through empirical study, it will shed light on the cybersecurity topics that individuals predict they cannot cope with alone and are induced to seek support available to them. Additionally, the work examines some possible shortcomings and threats of informal cybersecurity support. The focus is on the situation of Estonian citizens, further narrowing to the population who speaks Estonian or at least comprehends it in written form. By doing this, the thesis seeks to provide actionable insights for policymakers to address the cyber resiliency of the population. However, it endeavours for more generalisable outcomes since governments worldwide are digitising their services[2] and adversaries in cyberspace care little about geographical-cultural borders.

A notable contribution is the questionnaire developed during the research and the translation of the human cyber resiliency scale [40] into Estonian. Cybersecurity educators, including teachers and the youth police, could leverage it to pinpoint knowledge gaps within their audience, thereby enhancing the effectiveness of their teaching. Specifically, comparing teachers' responses to certain items of the questionnaire (Q7, Q8, and Q9) with those of

[2]For instance, the EU Cybersecurity Strategy for the Digital Decade aims for "100% of citizens having access to medical records" by 2030 [39]. Considering this, ensuring secure and privacy-preserving access to cybersecurity support is imperative.

pupils allows teachers to assess how accurately they predicted pupils' receptiveness to improvement on specific topics.

The current contribution tackles cybersecurity from the point of view of a home user. No distinction between safety and security is made here; rather, it uses the latter to encompass both terms. For individuals, the main concerns are the availability and integrity of their digital assets and the confidentiality of their private data. Whether these are threatened by a natural disaster (unintentional harm) or an adversary (intentional harm) is of minimal importance. While the nature of the threat is useful for experts who are crafting countermeasures, a layman merely uses the countermeasures recommended by experts. One can see similar usage of terms in the 2016 European Union scoping paper that defines: "cybersecurity refers to the protection of networks and information systems against human mistakes, natural disasters, technical failures or malicious attack" [41]. One can think of an individual being "cyber secure" while having peace of mind regarding the digital assets belonging to them or data about them in the possession of public and private sector organisations.

In the present work, cybersecurity, cyber resilience and digital privacy of individuals are handled. Such a broad scope is justified with the actuality that all these concepts are vital for the well-being of any individual who operates in digital environments. Cyber resilience has been explained as "the ability of the system to prepare, absorb, recover and adapt to adverse effects, especially those associated with cyber-attacks." [42]. This view has inspired setting the goal of citizen-centric cyber resilience as "to minimize the adverse impacts of cyber threats, enable citizens' continuous cyber functioning under and post-adverse cyber events, and to build the capacity to recover from and better adapt to adverse cyber events." [43]. When cyber resiliency refers to effectively recovering from problems in cyberspace while cybersecurity is practising cybersecurity techniques for securing one's devices, online accounts and data [44]. To differentiate between digital privacy and cybersecurity, it is noted that digital privacy is the right to control how one's digital data is used and controlled. In contrast, cybersecurity addresses measures how to protect that data.

The underlying idea under the work – to study Estonian home users' coping with cybersecurity issues via the phenomenon of cybersecurity caregiving – comes from the author. The author's contributions include searching for and reviewing relevant literature, gathering data and analysing, interpreting and translating it, and writing all sections of the thesis. Both study instruments were also designed by the author, with one exception. The survey questionnaire incorporated the human cyber resiliency scale, initially developed in English [40]. Translating the scale into Estonian was part of the current contribution.

The translation process involved the author and one of the supervisors. In addition to providing valuable feedback and inspiration, both supervisors assisted in narrowing down the scope, phrasing the research questions, calibrating the survey questionnaire (choice of items, wording), and guiding the analysis and interpretation of the quantitative data.

The rest of the thesis is structured as follows. An overview of the literature relevant to the current study is presented in Chapter 2, followed by the description and justification of the chosen methodology in Chapter 3. The design and execution of both research phases are given in subsequent Chapters 4 and 5. Data analysis results from the second phase are presented in Chapter 6, while the research questions are answered and discussed in Chapter 7. Limitations of the current work and possible future work directions are also outlined there, followed by the summary in Chapter 8. References and Appendices are the final parts of the thesis.

2. Literature Review

Literature relevant to the current study was queried mainly from Scopus and Google Scholar, some items were found from ACM Digital Library. The search string combined both, *cybersecurity* and *cyber resilience* with *citizen*, *home user*, *individuals*, *tech caregiving*, *support*, and *informal*.

The selected items explore the characteristics of home context, the correlation between awareness and behavioural outcomes, the phenomenon of tech caregiving, and existing cybersecurity support services or initiatives implemented internationally. Several authors point out that, compared to organizations, the cybersecurity of home users tends to get much less attention in academic literature [32], [45], [28], [46]. Breaches affecting home users get attention mainly when their devices or they themselves are involved in an attack affecting an organisation or critical infrastructure, e.g. the attack on Dyn [45].

Home context. Home context differs from work context in three main aspects that influence the security posture of its assets and users: the profile of users themselves, environment, and responsibility [32]. While users in the work environment are adults prepared for this work, home users are of all demographic groups with very varied online habits and cybersecurity awareness. The attack surface in the home environment is vast, comprising a wide range of devices connected to the Internet, including home-specific Internet of Things devices (baby monitors, smart watches and rings, security cameras, and other smart home gadgets) [47]. Responsibility between the home user and information technology provider is diffused [45]. Employees benefit from professional IT and cybersecurity training, policies, and support. This is usually not the case for home users in the challenges they face. Additionally, while the boundaries of responsibility are clear in organisations, at home, it is often unclear who is responsible for which device, service, or action. It is acknowledged that home users who learn cybersecurity skills at work likely implement them in the home context to some extent.

Relationship between awareness and actual behaviour. Awareness of cybersecurity best practices and risks does not necessarily lead to actually practising cyber-aware behaviour guidelines and applying countermeasures. This was shown more than a decade ago [48], and it holds despite society becoming more and more dependent on the internet [28], [49]. The same applies to privacy and is known as the privacy paradox. Prioritisation of business processes, limited resources and knowledge vacuum are the barriers to implementing

cybersecurity in small-scale IT users, including individuals [30]. Small-scale IT users value availability over confidentiality. They operate in situations where one human must undertake many roles, and cybersecurity expert is just one of them. When the budget is small, risks must be quantified, but quantifying risks imposed by cybersecurity threats is challenging in the home context.

Risk perception is crucial in forming individuals' understanding of the appropriate response to a threat [49]. However, only "personal relevance embodied in" the risk leads to a willingness to change behaviour and actual deeds. To practice security, people seek evidence of a security problem like direct harm to someone [28]. For identifying security problems, home users rely on intuition and visible signs (alerts, warnings, harm); they understand risks based on the perceived gain of the attacker and the perceived impact of an attack [45]. When their current security mechanisms fail to convey knowledge of an attempted or successful incident, they consider their security practices as sufficient [45]. Hence, the challenge of public awareness campaigns is that it is difficult to phrase messages conveying personally relevant meaning to all citizens. A study [50] has found that people's perception of risks on a national level is not shaped knowledge of actual threats, their origin, means, and purposes, rather by what media reports of attacks in other countries.

A strategy of getting help – tech caregiving. Googling does not necessarily lead to useful help since it floods users with a wide range of advice with uneven levels of credibility and relevance [51], [29]. Home users seek help from another source that is available when needed – their informal social networks [28] or tech caregivers [34], [35], [52]. Tech caregivers have been referred to as *CyberGuardians* in certain initiatives [53], and tech caregivers in an organisational setting have been described as *protective stewards* [54]. Tech caregivers have been identified from all age groups and sexes, and the same holds for tech caregivees; a person can carry both roles: caregiver and caregivee [34]. However, a tendency has been found that tech caregivers are from younger age groups with lower incomes, while older populations with higher incomes are often tech caregivees [35].

During tech caregiving sessions, privacy and cybersecurity are not addressed separately from general IT support issues; rather, these questions are raised in the context of more general support-related duties [34], [28]. Tasks that are performed by tech caregivers include troubleshooting, device or application setup [34], [28], new device or application explanation, adjusting settings, giving suggestions [35]. Coordination of support between tech caregivers and caregivees takes place mainly via text messages and phone calls [34], [35, 28].

Home users seek support from friends and family even if their expertise is irregular and the tech caregiver is only perceived as competent without necessarily being so [28]. Instead, continuity of care is a crucial characteristic of security support in the home: a valuable source of assistance is constantly available when needed. (This reflects how support is offered in organisational settings: in addition to training and awareness-raising practices, support personnel is available to help with issues, monitor the network and configure network devices.) The most preferable sources and targets of unsolicited help are also family and friends, followed by work colleagues [28].

Tech caregiver-caregivee relationships induce challenges since they can create negative emotions for both parties. Tech caregivees can feel disappointment, anxiety, or stress when the helper is unavailable, guilt for using the helper's time, or embarrassment for disclosing their problems. Helpers have reported frustration, impatience, and annoyance [52]. To cope with the relationship and handle emotions, tech caregivees have developed maintenance strategies such as avoidance or postponement. When giving access to one's device or account, users do perceive risks like loss and leakage of personal information, misuse of shared information, device or account, or change in relationship, but this may not make them take any access control measures like changing password [37].

When starting this research, academic research on tech caregiving, cybersecurity caregiving or informal cybersecurity support networks in Estonia could not be identified. During the writing of this work, an opinion that all Estonians would be educated in cybersecurity issues if every IT-savvy person here would educate three of their less tech-savvy peers [55]. This is essentially a call for practising cybersecurity caregiving. Also, during the compilation of this study, [56] was published describing librarians of public libraries in the Baltic states helping their readers with cybersecurity issues in reading rooms.

Situation of individual cybersecurity in Estonia. The Information System Authority (RIA) is the agency that ensures the cybersecurity of the Estonia [57] and provides regular overviews of the situation in cyberspace [58]. Their 2023 yearbook [59] outlines that cybercriminals finagled Estonian people more than 8 million euros and compared to 2022, there were 2.5 times more scams registered in 2023. Phishing, account hijacking, fraud and data breaches were the top incidents affecting citizens, with (mostly social media) account hijacking being reported 263 times. Effective phishing tactics involved the deployment of deceptive hyperlinks leading to counterfeit web pages closely mirroring authentic platforms (such as a courier website), disseminated to targets through emails or short messaging service (SMS) [59, pp. 11-12], or games that allow microtransactions [59, p. 22]. The situation of the citizens' cybersecurity in Estonia in 2023 is discussed in the interview of two cybersecurity experts of the State Information Agency [60].

The yearbook summarises the “Information Technology In Households" survey conducted by Statistics Estonia that highlights the annual increase in the reported cyber awareness of residents evidenced by implementing stronger passwords and inspecting links and attachments received from unknown senders [59, p. 43]. The survey asks questions about security-aware behaviour on the Internet, such as enhancements to one’s cybersecurity posture, activities to keep minors safe online and avoidance of e-services (public and commercial) due to security reasons [61]. Upon composing the current report, however, from the security-related questions, solely outcomes pertaining to respondents’ understanding of cookies and their limiting in web browsers were published in their statistical database [62].

Formation of cybersecurity-related behavioural habits. According to [63], factors influential to home data security decision-making fall into categories such as motivation, capability, context, and perception. Beliefs about capabilities and consequences, reinforcements, social influences, social/professional role, identity, and emotions influence individuals’ cybersecurity behaviour [64]. This suggests that besides knowledge and skills, considering (organisational) culture in awareness initiatives would enhance their effectiveness. The benefit of securing and the cost of not securing one’s smart home network had “significant effects on an individual’s attitude towards performing security behaviours” [65].

One construct stands out as constantly predicting security behaviours: self-efficacy [65], [33], [64], [66], [34], [35], [67], [68]. Self-efficacy is "an individual’s perceived personal capacity to complete a task" [34] showing "whether a person believes that they can successfully execute the behaviour required to produce the desired outcomes" [67, p. 9]. When looking for the driving factors impacting an individual’s intention toward performing security behaviour, [65] identified relationships between the cognitive and psychological factors and individual security intentions. Besides awareness of threats, self-efficacy correlated with an individual’s intention to secure their smart home network. Self-efficacy is shown to be positively influenced by situational support (that is, individuals helping each other, assistance from a supervisor or colleagues, having time allocated for practising behaviours) [66]. This suggests that the supportive environment is a mechanism that reduces the pressure on the non-expert to find a solution when a cybersecurity incident occurs [69].

Another notable construct is power usage: “an individual’s propensity to be a proactive technology user that explores all customisation options” [34, p. 396:2], as cited from [70]. Compared to tech caregivees, tech caregivers report significantly higher levels of power usage [34], [35]. On the other hand, user anxiety, openness to social support, self-efficacy, and security awareness are variables predicting willingness to receive support [71].

Proposals and challenges of improving cybersecurity posture in the home context. Taking cultural and human aspects into consideration, as advocated by [38], underscore the importance of cybersecurity culture, which extends beyond mere awareness to encompass an understanding of risks and procedures to avoid these. Two research groups, Kropczynski et al. and Nthala et al. have published the most comprehensive studies on tech caregiving, respectively [34] and [28], [45]. Based on their findings, both groups propose that the security situation of the home can be improved by targeting interventions at the support network rather than the end user directly for two reasons. First, the change is encouraged at the point where security work will most likely materialise. Second, users will acquire both security knowledge and skills in this way. Competence-building should address tech caregivees' capability to initiate caregiving sessions on cybersecurity and digital privacy and educate them on engaging in digital privacy and security discussions. This proposal is justified by the finding that helpers do not necessarily possess the technical or communication skills to assist efficiently [72]. The observation that tech caregivers' motivation fades over time calls to find mechanisms to encourage them to continue providing support beyond the initial setup. Removing agency from individuals by security by design or strict cybersecurity policies is suggested as a more effective cybersecurity method than messaging campaigns that shift responsibility to users [49].

However, how to increase home users' ability to assess the quality of a security decision, source of support, or product remains the main challenge in this regard [28]. How should a home user confidently distinguish between a genuinely competent and an incompetent helper (despite their consciousness of the fact)? How should they recognise a malicious attacker impersonating a friendly helper?

3. Research Design

The choice of methodology, its justification and accompanying ethical aspects are covered in this chapter.

3.1 Methodology

To approach the problem described in the Introduction, mixed methods research executed in subsequent phases was chosen [73, Chapter 27]. In an interdisciplinary setting where comprehensive research is not yet available, mixed methods is used to benefit from the integration of qualitative and quantitative methods. Citizens' needs for cybersecurity support, tech caregiving in the cybersecurity domain and the risks it may bring about have not been researched in Estonia. Qualitative methods are developed to gain a deeper understanding of a phenomenon and get more nuanced insights into new study areas. They are often used for exploring a field that lacks theory or where comprehensive research has not yet been conducted [74]. Results of the first phase utilising qualitative methods would contribute to the work in two ways. They help discover acute problems or important aspects of the phenomenon that are not examined in the existing literature. This potentially leads to refocusing the research through a review of the research questions. Secondly, they would inform the creation of the study instrument for collecting quantitative data. Knowledge of the subject area and challenges there is a precondition to working with quantitative data. Once this precondition is met, quantitative methods enable to aim for generalisable results.

The initial phase would involve gathering firsthand insights into the state of cybersecurity support for laypeople in Estonia from field experts. Following their knowledge, research questions would be reviewed to be better served by the qualitative and quantitative methods. Then semi-structured interviews would be conducted to get insights into the cybersecurity caregiving phenomenon in Estonia and map typical cybersecurity topics and incidents that laymen have experienced here. The author decided to approach the subject matter through the eyes of cybersecurity caregivers instead of home users themselves. The benefits of involving cybersecurity caregivers are two-fold. They would inform the research about what questions their cybersecurity caregivees ask them, what cybersecurity caregivers consider important topics in home users' cybersecurity behaviour, what is their overall impression of the status of home users' cyber hygiene and what tactics they see as successful for improving it. Another effect of talking to cybersecurity caregivers is related to terminology

and language. Cybersecurity is too young a domain to have all language speakers adopt the same terminology to refer to domain-specific phenomena. This infers that a study participant and the researcher might use different words. A home user might even have no words to describe a specific cybersecurity incident or situation. Thus, the cybersecurity caregiver acts as an intermediary or translator between the researcher and cybersecurity caregivees, providing the former words to use in survey questions. To prevent further misunderstandings arising on language use, the whole study would be conducted in one language only: Estonian.

To mitigate acquiescence or agreement bias, the interview guide would include several open-ended questions, and leading questions would be avoided. Questions would be carefully worded and ordered to minimise the effects of habituation and question-order biases. The researcher would keep the interview atmosphere respectful, and the participants would be assured the results would be published anonymously without assessing their or their caregivees' reported behaviour to minimise the social desirability bias. Naturally, this promise would be kept while writing and defending the thesis.

Based on the findings from the thematic analysis of the semi-structured interviews the research questions would be refined and the study instrument for the second phase developed [73, pp. 643-644]. This means the choice of situations for the web questionnaire, wording of questions and invitation distribution plan. The survey is aimed at all adult citizens and residents of Estonia who are able to respond to a questionnaire in the Estonian language. After analysing the survey data, the research questions would be answered by integrating the results of both phases of the study. Following a triangulation protocol [75], [76] would show where the results from each method agree, contradict or add to each other. Disagreement between findings is not a sign of failure, instead, investigating discrepancies offers an opportunity to better understand the problem.

3.2 Ethical Considerations

For the current study, adult Estonians will be the main sources of data. Since the data will be gathered in Estonia, the General Data Protection Regulation (GDPR) and the Personal Data Protection Act [77] apply. In the course of the communication with the interviewees, recording of their voices, their contact information, as well as unpredictable personal data, will accumulate under the custody of the researcher. To ensure this data is handled according to the regulations,

1. the interviewees will be asked to sign an informed consent form after the aim of the study and their rights have been introduced;

2. for transcribing the interview recordings, a locally installed transcription software is preferred over a cloud-based one;
3. before responding to the survey questionnaire, the participants will be informed to not disclose identifiable personal information about them or anyone else;
4. the researcher will establish and follow a data management plan defining details of access, storage and backup, and deletion of all types of personal data gathered:
   (a) interview recordings and transcriptions,
   (b) signed consents,
   (c) written communication (e.g. e-mails),
   (d) survey data;
5. only such identifying information is asked from data sources that is inevitably needed for answering the research questions. This applies to both interviewees and web survey respondents.

The fact that in the thesis, the results will be presented in a pseudonymous or anonymous form will not relax the GDPR requirements. In all phases of the research, especially during the interaction with the interviewees and presenting the results, a neutral attitude has to be maintained and judgements avoided. The interviewees have the right to withdraw their consent and ask the researcher to exclude their data from the data set. Should any respondent exercise this right, the data set for analysis becomes smaller by the time of submission. The author has to take time to handle such a request.

4. Phase One. Interviews to Explore Cybersecurity Caregiving and Needs for Cybersecurity Support in Estonia

The study set off with contacting the analysts of the Estonian State Information Authority working on cybersecurity prevention activities and cyber awareness of the population. The aim was to explore the situation of cybersecurity support for Estonian home users and to understand in which way the current research could contribute. Drawing from these consultations [36], RQ1 was specified to collect the cybersecurity topics or domains where support is needed. They also underscored their lack of comprehension regarding variations in needs among demographic groups (RQ5). An interview guide (Appendix 8) and an informed consent form were the study instruments created for this phase.

4.1 Recruitment and Interview Procedure

Interviewees had to meet the following criteria. They had to be adults, citizens or residents of Estonia and provided cybersecurity-related informal support to at least one caregivee in 2022 or 2023. Participants were recruited by asking the author's acquaintances to recommend qualifying individuals. The interviewing period started in January 2023 and lasted until the end of October 2023. Interviews took place, upon the interviewee's preference, in the form of video calls in Zoom environment or face-to-face meetings. Balancing the need for saturation of information with the time available, seven interviews were conducted altogether, resulting in 297 minutes of recorded material. The mother tongue of all participants was Estonian, and they were employed at the time of the interview. Table 1 shows the participants' demographics.

The interview guide was not adhered too rigidly, allowing the conversation to move on to topics that were important to the interviewees and in the order in which these logically emerged. Interviews started with the introduction: an explanation of the purpose of the study and how the interview contributes to it, the participant's rights, agreement on recording, and an explanation of central concepts and terminology. When the demographic data of the participant was recorded, all interviews continued with looking iteratively into cybersecurity related incidents/events that the interviewee had assisted in solving in recent years (Question: "Have you assisted anybody in a cybersecurity or privacy-related incident during 2022 or 2023? If yes, let's look at them more closely one by one."). The next block of questions was about participant's preventive activities to enhance their cybersecurity caregivees' cybersecurity or introduce cyber hygiene best practices. Later on,

Table 1. Interview participant (n=7) demographics (Phase One).

Demographic	Category	n
Age	18-34	4
	35-64	3
	65+	0
Gender	Male	4
	Female	2
	Other	0
	Prefer Not Disclose	1
Education	Primary school (9 yrs)	0
	Grammar school	1
	Vocational education	1
	Undergraduate	2
	Graduate	2
	PhD	1

the participant was encouraged to reflect on their experiences with cybersecurity caregiving and how they related to this phenomenon. Time permitting, more general topics were discussed: cybersecurity awareness among laymen in Estonia, the participant's concerns about cybersecurity situation of home users in Estonia, characteristics of vulnerable population segments, impactful countermeasures that would, when adopted by the whole population, make the most significant change for better cyber resilience. Once the interview was over, the participant was thanked for contributing their time. No reward was offered to them.

Audio recordings were transcribed using Kaldi Offline Transcriber [78], and transcripts were edited manually to correct speech recognition errors. Transcriptions were then coded, codes written out to a separate file, and organised into recurring themes and categories for subsequent use in survey preparation. The transcripts were then reread, bearing these themes in mind, looking for and extracting any new codes that had been previously missed. The method of thematic analysis typically involves the collaboration of multiple researchers to enhance objectivity through independent coding. However, to meet the master's thesis requirements, the author conducted the analysis of the interview transcripts independently.

4.2 Analysis and Findings

As a result of the thematic analysis of interview transcripts, the author identified two themes: *Support* and *Concerns*. *Support* refers to a cybersecurity caregiving session discussed in the interviews (see Table 2). *Support* was further divided into two types – *Reactive* and *Proactive*, depending on the session's initiator. *Reactive Support* includes situations where the support session is initiated by the cybersecurity caregivee who faces a cybersecurity

event, incident, or question. On the other hand, when the cybersecurity caregiver starts the session, *Proactive Support* takes place. The trigger for this can be their observation of the risky behaviour of the cybersecurity caregiver, a questionable configuration of their device or wish to share information, news or their inner understanding about a change needed. The author further divided both types of *Support* into categories/characteristics of *Topics*, *Timing*, *Strategies*, and *Principles*. The category labelled *Topics* refers to cybersecurity-related issues and questions that the cybersecurity caregivee asks from their cybersecurity caregiver or recommendations that the cybersecurity caregiver informs their cybersecurity caregivee about. *Timing* indicates the time or situations when cybersecurity support occurs. With *Strategies* the author considers the activities that constitute a support session. The category *Principles* denotes the inherent guidelines formulated by the cybersecurity caregiver to adhere to during the cybersecurity session.

Table 2. Theme *Support* and its classification into categories as derived from the thematic analysis of interview transcripts.

Type	Reactive Support	Proactive Support
Topics	account hijacking, phishing, device inspection, privacy and security settings, good passwords, security and privacy of platforms, confusion from different PIN codes	phishing, multi-factor authentication, password management, good passwords, ad blocker, open source software, privacy-invasive apps, screen lock, encrypting-decrypting files, DigiDoc client, i-voting and verifying vote
Timing	during or right after recovering from an incident, during general IT support	when visiting caregivee, at dinner table, at Christmas, upon caregiver's experience of a threat
Strategies, activities	diagnosing, recovering, inspecting, configuring, reporting, encouraging self-sufficiency by providing keywords for googling; avoid touching cybersecurity caregivee's device, instruct to find solution themselves (rather than cybersecurity caregiver resolves the issue)	sharing info on social media, sharing articles/blog posts directly to caregivees, sharing personal experience (e.g., showing a recent phishing mail), device inspection, asking intriguing questions about preparedness to face a certain loss, disclosing cybersecurity caregiver's expertise in cybersecurity, party tricks
Principles	analysis security needs of cybersecurity caregivee (confidentiality, integrity, availability), explain from caregiver's point of view (not caregivee's), reject requests to hack	explain from caregiver's point of view (not caregivee's), promoting via threatening is unethical

The other theme, *Concerns*, incorporate challenges and problems as identified by the cybersecurity caregivers for maintaining better cyber hygiene and cyber resilience of the cybersecurity caregivee or the society (see Table 3). This theme was further divided

Table 3. Theme *Concerns* and its classification into categories as derived from the thematic analysis of interview transcripts.

Attitudes	convenience and features valued over security and independence; security is unpopular and not valued; defence is boring, offence is cool; "nothing to take from me" and what can be taken is protected by other means; lack of critical thinking, also among extensive computer users
Practices and lack of practices	smartphones used with default settings, awareness is not doing - how to make people really practice cyber hygiene, real damage via an incident is the only thing that may make to implement a countermeasure, adoption of password managers and passphrases would make huge impact, impulsive clicking
Inevitabilities	the young lack experience needed to recognize suspicious mail/site/behaviour, no sources for laypeople to learn security, steep learning curve for adopting password manager
Consequences	citizens lose money/time/privacy; reputational damage to state

into categories that emerged from the interviews: *Attitudes* and Practices (and lack of practices) of laypeople, *Inevitabilities* and *Consequences*. Under *Attitudes*, information about laypersons' stances that hinder their cyber-aware behaviour was gathered. Under *Practices*, reports of activities and lack thereof are assembled that countermine the adoption of cyber security best practices. *Inevitabilities* are characteristics of a population segment, the current state of affairs in the society, or the nature of a countermeasure that cannot be ignored or overruled. *Consequences* specify the results that the population's weak cyber hygiene or low cyber resilience may have on society or the state.

An important finding from the interviews was that it is not only cybersecurity but also cyber resilience of the cybersecurity caregivees that cybersecurity caregivers are concerned about. Recovering accounts and recommending measures for fast recovery from cyber incidents is a common topic in their support sessions. This suggests that citizens' need for support to enhance their cyber resilience should also be addressed in the second phase of the research. The findings from the qualitative data are elaborated further in Appendix 2.

5. Phase Two. Developing and Executing the Survey

In this phase, quantitative data was gathered to facilitate answering the research questions. The chapter first describes creating a web survey based on the findings from Phase One and the literature. Second, it presents the study sample and the survey questionnaire validion.

5.1 Survey Questionnaire and Recruitment

A web survey among Estonian citizens was conducted to gather data for the quantitative part of the research. The following sections describe how the survey questionnaire was created, how the survey was conducted, and what the findings were.

Table 4. Outline of the survey questionnaire showing how specific survey questions, grouped into sections, contribute to answering the research questions.

Purpose	Section of Survey	Survey Questions
	Introduction.	
Profiling	Demographics.	Q1–Q6, Q13, Q17
RQ1	Asking help in situations of:	
	a) cyber events and incidents,	Q7, Q10
	b) cyber hygiene and situational awareness,	Q8, Q10
	d) transparency of personal data usage.	Q9, Q10
	Awareness of recommendations.	Q28, Q29
	Characteristics of cybersecurity related support:	
RQ2	a) desired,	Q11, Q12, Q14, Q17
RQ3	b) actual.	Q13, Q15–Q20, Q30
RQ4	Risky situations from informal cybersecurity support:	
	a) already happened,	Q17, Q21, Q22, Q24, Q26
	b) likely to happen.	Q23, Q24
Profiling	Individual cyber resilience.	Q27
RQ1	Awareness of 6 recommendations.	Q28, Q29
	Thank you.	

Findings from the interviews (Tables 2 and 3) supported by literature [59], [61] [28], [34], [52], [45], [16] informed the choice of topics for the survey and formulation of questions. For example, an interviewee saying they avoid touching the cybersecurity caregivee's device induced to consider the issue of (misuse of) trust that was also mentioned in [28]. Thus the question "When someone is helping you privately with cybersecurity, who enters the information into the device?" (Q21) was added to the survey. Another interviewee emphasising the impact of adoption of password managers on one's cybersecurity posture, inspired to include related items to the survey questionnaire (Q8). The flow of the resulting

questionnaire with the mapping of research questions to the survey questions can be followed in Table 4. For the full text of the questionnaire, see Appendix 3 for the survey in Estonian or Appendix 4 for its English translation.

Three approaches were utilised to profile the respondents. First, demographics such as age, gender, education, socioeconomic status, and time spent online were included in the questionnaire (Q1–Q6). The answer options for age, education, and occupation were chosen to align with similar questions in the household study questionnaires by Statistics Estonia [61]. The options for noting gender were inspired by [28]. Second, respondents' experiences with cybersecurity caregiving was also regarded as independent variables: whether the participant reports to have a cybersecurity caregiver (Q13).

Third, the human cybersecurity resilience scale [40] was included in the questionnaire as a third tool for participant profiling. This measure consists of 16 items in four subscales- self-efficacy, helplessness, social support, and learning and growth- and assesses individuals' ability to resist and recover from cyber attacks. The scale was translated into Estonian according to the following procedure. First, the author of the current thesis translated the scale from English to Estonian. Second, this Estonian version was translated back to English by another person who is fluent in English and familiar with the subject matter. Third, both persons involved compared and discussed the results, reaching a common understanding of the best wording. One author of the scale was consulted for details of running the scale, informing the exact wording of the introduction and prompt, and that the items should be presented to respondents in random order [79]. Finally, the result was piloted with four native speakers of Estonian, and the misunderstandings they pointed out were addressed.

Private life situations where one would ask for help (addressing RQ1) were asked in three thematic blocks: cybersecurity incidents and events, cyber hygiene and transparency of private data collection and usage. Additionally, awareness of six sample recommendations to solve cybersecurity tasks was added to the questionnaire to learn about situations where citizens struggle or, to the contrary, are competent. Next, the respondent was asked to select what qualities they value in cybersecurity-related assistance for private matters, followed by questions about their experience with cybersecurity caregiving (supporting answering RQ and RQ3). Problems arising from informal cybersecurity support in Estonia (RQ4) were addressed via possible vulnerable situations where a cybersecurity caregivee can find themselves when asking for informal support. The survey questions were built around account management and internet voting. While the former is a universal group of tasks, the latter is specific to Estonia, where legally binding nationwide internet voting has been used for elections since 2005. Approaching the question from two angles, the

past and the future, the questionnaire asked about the occurrence of a risky situation in the respondent's life and their estimation of the likelihood such situations might take place in years to come.

The resulting survey questionnaire consists of 31 questions. Among these, seven questions were used to profile the respondents: six were about demographics, and one was about individual cybersecurity resilience. Six free text fields were added, enabling respondents to clarify or comment on their answers. All questions were mandatory, apart from the free text fields. There were three forks where the answer determines the next question asked presented. For example, depending on whether the respondent has a cybersecurity caregiver (Q13), they are either asked to describe their personal experience with cybersecurity caregiving (Q15 to Q21) or indicate whether they wished to have someone to ask (Q14).

All main questions were multiple choice or single choice; free text fields were not mandatory. The latter was only added at the end of some questions where the author might have missed an important option or choice in the previous question. This way, extensive collection of qualitative data was circumvented, thereby enhancing the comparability of responses. Also, the risk that respondents accidentally disclose personal information about themselves or their cybersecurity caregiver was mitigated.

The questionnaire was created and published in the Estonian language. The wording of questions and answer options and the time needed for responding were tested in agile sprints with ten native speakers of Estonian, some of them cybersecurity experts. For the survey platform, the European Commission's web application tool for online survey management, EUSurvey [80] was chosen to guarantee participants' privacy. To achieve the anonymity of contributions, the survey was created in an 'anonymous survey mode' that prevents EUSurvey from saving any personal data and connection details [81].

Responses to the questionnaire were gathered from January 9th to February 5th, 2024. The invitation was sent to the administrators of mailing lists of several curricula of a university, a vocational school, and some community organisations with the request to forward it to the mailing lists under their moderation. It was shared on social media platforms and in an online forum. Also, the author's friends and colleagues were asked to disseminate the invitation among their peers, including the less IT-savvy population. However, the author did not request feedback about how much this request was followed for privacy reasons.

5.2 Demographics of the Sample

With the web survey, 161 responses were gathered (see Table 5). 51.55% of the respondents were female and 45.34% male, which resembles the ratio in the Estonian population [82]. Some people chose "Other" for gender or preferred not to disclose it. The age distribution of the sample is roughly similar to the age pyramid of Estonia [83]. However, the 18-24 years old participants are overrepresented in the study sample. The 35-44-year-olds form the biggest age group in the nation's population. Age distribution is similar between men and women (chi-square p=0.5).

Most respondents hold higher education degrees, followed by those whose highest completed level of education was grammar school. The proportion of education is distributed differently between men and women (chi-square p=0.006). There is a higher proportion of females with grammar school education (73.49%) than higher education (24.10%), while the situation is reversed for the men (34.25% and 58.90%, respectively). The sample was skewed towards the employed and students/pupils that comprised the biggest socioeconomic groups (64.84% and 19.26%, respectively). The age composition of socioeconomic groups reflects the natural state of affairs in the society, e.g., the majority of the 35–54 are employed and, among the young, many have still grammar school education.

Most respondents (approximately two-thirds) used 20 or more hours of Internet for work or school-related tasks, while for other than work/school-related tasks, the majority (also two-thirds) used 20 or fewer hours a week. Naturally, the employed and students report spending more time on the Internet for work/school-related tasks than the other groups (chi-square p<.001). Working people report using more hours of the Internet for work/studies than students. Compared to other education groups, the respondents with higher education tend to spend more hours on the Internet for work (chi-square p=0.045). Internet usage for other than work/school-related tasks was remarkably similar between employed individuals and students. There is no relationship between socioeconomic status and Internet usage for private matters.

Five-fourths of the respondents had a cybersecurity caregiver, and of them, almost two-thirds agreed that the support they received from them was currently sufficient. A larger access to a cybersecurity caregiver can be seen among the men in the sample compared to women. Compared to other groups, the young adults (33.82%) and students (41.94%) distinguish for a high proportion of respondents without a cybersecurity caregiver. Roughly half of those without a cybersecurity caregiver claimed they did not miss one, while the other half said they do. Approximately two-thirds of the students and of women admit feeling a need for a cybersecurity caregiver.

To increase the power of the analysis, age groups “65–74” and “75 or more” were merged into “65+”. Respondents who had chosen “prefer not to disclose“ or “other“ for gender were included in a new group “other/not known”. Similarly, less represented educational groups, such as vocational and primary education, were aggregated with responses from those who preferred not to disclose. The recruits, unemployed, housewives or -husbands and the retired were aggregated as “other”. Table 5 reflects the demographics before merging.

Table 5. Survey participant (n=161) demographics (Phase Two).

Demographic	Category	n	Percent
Age	18-34	42	26.09%
	25-34	26	16.15%
	35-44	29	18.01%
	45-54	36	22.36%
	55-64	16	9.93%
	65-74	8	4.97%
	75+	4	2.48%
Gender	male	73	45.34%
	female	83	51.55%
	other	2	1.24%
	prefer not to disclose	3	1.86%
Education	primary school 9 yrs	1	0.62%
	grammar school	46	28.57%
	vocational education	5	3.1%
	higher education	107	66.46%
	prefer not to disclose	2	1.24%
Socioeconomic status	employed	106	65.84%
	unemployed	6	3.72%
	retired	9	5.59%
	pupil or student	31	19.26%
	housewife/husband	5	3.1%
	recruit	4	2.49%
Hours Internet for work/school	up to 10h	32	19.88%
	11–20h	26	16.15%
	21–40h	60	37.27%
	41+h	43	26.71%
Hours Internet for other than work/school	up to 10h	39	24.22%
	11–20h	67	41.61%
	21–40h	38	23.6%
	41+h	17	10.56%
Has cybersecurity caregiver	yes	129	80.12%
	no	32	19.88%
Current informal support sufficient (n=129)	yes	95	73.64%
	maybe	30	23.27%
	no	4	3.01%
Expressed need for cybersecurity caregiver (n=32)	yes	15	46.88%
	no	17	53.13%

6. Survey Results

This section will answer the research questions phrased in the Introduction. First, the validity of the survey questionnaire and the quality of the survey data will be assessed. Then, the results of the qualitative study will be analysed, and the research questions will be answered by integrating the findings from all phases of the work.

6.1 Validity of the Questionnaire and Data Quality

The validity of a study instrument means an assessment of how much it measures what it is intended to measure [84, p. 7]. First, data gathered via free text fields that followed multiple-choice questions were examined to judge the validity of the questionnaire created and used in phase two. Indicating a weak design would be many additions in these fields, showing that respondents felt a comprehensive answer was impossible with the options provided. Then instances where respondents did not understand the question were looked for.

In the survey, free text fields were Q10, Q12, Q16, Q20, Q24, and Q31. Eight respondents out of a total of n=161 (4.9%) used the possibility to add to Q10 and Q12, and five or fewer participants filled other free text fields. This indicates that most respondents found a suitable set of answers. The feedback collected from these fields is reported together with the analysis of the respective questions.

Respondents' confusion indicates a poorly phrased question that potentially delivers ambiguous results. Survey questions with a "Do not understand" option were Q7–Q9, Q21, Q26. In Q7–Q9 ("In which situations would you ask another person for help or advice?"), such answers were included intentionally to point at cybersecurity topics unfamiliar to the respondents. As such, they directly contribute to answering RQ1 and are interpreted in the next section. For Q21 ("When someone is helping you privately with cybersecurity, who enters the information into the device?"), this option was ticked by 11 people (8.5% of n=129), and it can be agreed that it really indicates puzzling wording here. Only one respondent out of n=137 did not understand the statement, "Someone has coerced me at i-voting." (Q26). The above discussion leads to a positive assessment of the validity of the study instrument, provided the results of Q21 are regarded with care.

Feedback from early respondents made the author change the answer options for Q7–Q9.

This induced the exclusion of the 14 first responses, leaving n=147 valid records for Q7–Q9. No other items of the questionnaire were affected. Due to a misleading translation discovered in the human resiliency scale after the closing of the survey, the usage of this study instrument had to be discarded altogether.

6.2 RQ1: In which Cybersecurity-related Situations Would Estonian Home Users Ask for External Advice?

The answer to RQ1 was a list of situations or topics. RQ1 was first addressed by asking the survey participants an overarching multiple-choice question, "In which situations would you ask another person for help or advice?" The 22 items (situations) were grouped under incident handling (Q7), cyber hygiene and cyber situational awareness (Q8), and transparency of private data usage (Q9). After that, Q10 enabled the participants to add any situations or topics that they missed in Q7, Q8 or Q9. Approaching the research question from another angle, the knowledge of six cyber hygiene recommendations (Q28) and whether the respondents felt they were able to utilise one of these (Q29) were asked.

The answer options for Q7–Q9 were "Would ask immediately", "Would ask if a quick search on the Internet does not lead to a solution", "Would ask if a thorough search on the Internet does not lead to a solution", "Would not ask even if I cannot find a solution", "Would not ask because I know what to do / because I can do it", "Do not understand the question". The three "Would ask..." questions were aggregated because they all express a need for external help. The urgency aspect was ignored since whether a person reaches out for help sooner or later also depends on personality, not solely on the nature of support available. Responses "Do not understand" likely signal an unknown topic.

There were seven respondents who used the option to select "Do not understand the question". All other participants answered all the questions, suggesting that most respondents generally understood the questions well. Of the 22 sub-questions, 12 received one or more responses "Do not understand the question". The items that were the least familiar to the respondents were Q7d, Q8a, and Q8i, which received four such answers.

Table 6 presents the ranking of the 22 items by the count of responses to all three "Would ask..." questions and "Do not understand the question" combined. The first five items fell into maintaining cybersecurity situational awareness and cyber incident management categories. All 22 proposed situations received a "Would ask..." or "Do not understand" response by at least 42% of the respondents showing that none of these cases was trivial.

Table 6. Results of the survey questions Q7–Q9. The items (situations) are ranked by responses (n=147) to "Would ask..." and "Do not understand the question" combined.

Rank	Item	Ratio
1.	I need to find out if my device has been compromised. Q8j	88.44%
2.	I need to find out if any of my home devices (e.g. security camera, baby monitor, etc.) are being used in a cyber attack. Q8k	87.08%
3.	My files won't open, and I see a message saying these are encrypted and money asked. Q7f	79.59%
4.	I need to monitor traffic passing through my home router. Q8i	74.83%
5.	I can't log in to my email account and suspect it has been taken over. 7b	71.43%
6.	I want to report a cyber threat or crime (e.g. phishing campaign, cyber-bullying, identity theft). Q7e	68.71%
7.	I want to know what data some of my devices collect and share. Q9d	68.03%
8.	I can't sign in to my social media account and suspect it has been taken over. Q7a	67.34%
9.	I want to know which data in Estonian registers and information systems I have consented to use. Q9b	66.67%
10.	I need to change my home router's visibility, name or password.Q8h	65.31%
11.	I want to know what consents I have given to third parties for using my data in web browsers. Q9c	62.59%
12.	I want to limit inappropriate data collection on my devices and apps. Q9e	61.22%
13.	I entered my PINs on what could have been a phishing website. Q7c	61.22%
14.	I want to know who has requested data about me from Estonian e-government databases (Health Information System, e-Tax Board). Q9a	60.54%
15.	I need to find out if the website I am entering my data on is secure enough to do this. Q8g	59.86%
16.	When signing in with Smart ID or Mobile ID, my phone displays a different verification code than the webpage from which I initiated the process. Q7d	57.82%
17.	I need to understand the security settings of my device/account. Q8d	57.82%
18.	I need to encrypt a file containing sensitive information in the name of the recipient. Q8c	55.78%
19.	I need to find out if this is a safe email or message. Q8f	55.78%
20.	I need to find out if this is a safe link. Q8e	55.10%
21.	I need to start using a password manager. Q8a	53.06%
22.	I need to set up MFA for my most important accounts. Q8b	42.18%

The majority of respondents who would not seek help reported knowing a solution. The items that were familiar to the biggest proportion of respondents come from the domain of cyber hygiene: setting up multi-factor authentication (Q8b, 51.55%), adopting a password manager (Q8a, 41.61%) and encrypting a file in the name of the recipient (Q8c, 40.37%). On the contrary, the smallest proportion of respondents can be seen knowing how to detect whether one's device has been compromised (Q8j, 6.48%) or used in a cyber attack (Q8k, 7.87%) or what to do when falling victim to ransomware attack (Q7f, 12.96%). Finding an

email account inaccessible (Q7b) or being in need to encrypt a file in the recipient's name (Q8c) were items where nobody selected the option "Would not ask even if I cannot find a solution". The number of responses indicating ignorance of the problem ("Would not ask even if I cannot find a solution myself") did not reach 5% for most items; only Q9d (11.18%) and Q9c (9.32%) stood out for more considerable proportions.

The topics that people are most ready to invest effort to find a solution on the Internet on their own are interesting from the aspect of suitable channels for support. Items that made a remarkable share of respondents tick "Would ask if a thorough search on the Internet would not lead to solution" are where people would first google. Thus, easily discoverable and usable online resources would have the most considerable effect. The results of the survey show that such situations are

1. I want to know which data in Estonian registers and information systems I have consented to use. Q9b (32.30%)
2. I want to know what consent I have given to third parties for using my data in web browsers. Q9c (31.06%)
3. I need to monitor traffic passing through my home router. Q8i (29.19%),
4. I can't sign in to my social media account and suspect it has been taken over. Q7a (28.57%), and I need to find out if the website I am entering my data on is secure enough to do this. Q8g (28.57%),
5. I need to find out if any of my home devices (e.g. security camera, baby monitor, etc.) are being used in a cyber attack. Q8k (27,95%),
6. I want to know what data some of my devices collect and share. Q9d (27.33%).

The free field responses to Q10 brought five new topics, of which backup management was mentioned twice (e.g., "I need to set up a backup system for my home computer or device."). Topics mentioned once included restoring forgotten passwords, discovering an unknown device in the network configuration of one's computer, and assessing software safety. One respondent wanted to know what data about them and for which purposes online platforms/portals collect, hold, and use; and from where it was collected.

To see which cyber hygiene recommendations provided in Q28 have not been adopted by the respondents, the author counted the answers "First time I hear about it". Checking a link or an attachment in a dedicated virtual environment or sandbox scored the highest (Q28b, 61%). Checking the link by hovering over it followed (Q28c, 36%). In the following question, Q29, the respondent was asked whether they could check the safety of the links provided in these recommendations. Even after reading the recommendations, 16.15% of the respondents were unsure, indicating it by selecting "No".

6.2.1 RQ5: How Does the List of Situations where Estonian Home Users Would Seek Cybersecurity Advice Depend on Sociodemographic Variables or Internet Usage?

The chi-squared test was utilised to identify sociodemographic variables that have an effect on the distribution of answers for Q7–Q9. The chi-square value shows how much the distribution of answers within a group (defined by a categorical variable) differs from one group to another. A low p-value indicates that there is a significant association between these variables. Considering the number of responses, a p-value below 0.05 is regarded as showing a significant effect, while $0.05 \leq p < 0.1$ indicates a marginal effect. Table 7 summarises the significance of the impact of sociodemographic variables on the distribution of responses to Q7–Q9.

Having a statistically significant effect on all items except for Q9a and Q9b, gender emerged as the most influential variable. It was followed by Internet usage for work/school-related tasks (impacting sixteen items statistically significantly, two marginally) and sociodemographic status (statistically significant effect on eleven items and marginal on two items). The least influential were Internet usage for tasks other than work or school and the existence of a relationship with a cybersecurity caregiver.

Gender. The proportion of men who reported they knew a solution was consistently more significant than that of women for the same question. Also, the distribution of responses given by men was uniform across all questions, whereas the distribution pattern varies among women. For all questions, proportionally more women would ask for advice (or did not understand the question), and fewer reported they knew the answer. Extreme cases were Q8j and Q8k, for which no woman stated they would avoid asking because they knew what to do. More than a fifth of male respondents claimed the opposite for the same question.

Internet usage for work/school related tasks. Comparing the groups revealed a general trend (with some exceptions) that as the number of hours increases, the proportion of respondents within the group who claim to know a solution also rises. The fewer hours, the proportionally more respondents who would reach out for help. Among individuals spending 41+ hours on the Internet, there were never fewer respondents who reported knowing the solution than those who would ask for assistance; in some cases, the numbers were equal. A substantial majority (ranging from 65.39 to 92.86%) of individuals who use the Internet 0-20 hours per week for work/studies would seek assistance at some point. Among them, only up to one-third would know what to do in these situations (exception:

Table 7. Chi-square p values identifying the significance of the effects of sociodemographic variables or Internet usage on the responses (n=147) to Q7–Q9. Values $p<0.05$ are in bold to mark statistically significant effect. Values $0.05 \leq p < 0.1$ indicate where the statistical significance of the effect was marginal. Age groups 65–74 and 75+ were consolidated into a single group, while groups in other demographic variables were merged according to the descriptions provided in the Demographics of the Sample section.

Question	**Age**	**Gender**	**Education**	**Socioeconomic**	**Internet for Work**	**Internet for Other**	**Has Cyber Caregiver**
Q7a	0.2	**<.001**	0.37	**0.03**	**0.002**	**<.001**	0.2
Q7b	0.09	**<.001**	0.09	**0.03**	**<.001**	0.07	0.4
Q7c	0.21	**<.001**	0.07	**0.02**	**<.001**	0.4	0.9
Q7d	0.2	**0.004**	0.54	0.13	**0.01**	0.3	0.5
Q7e	0.09	**0.017**	0.62	**0.017**	0.41	0.92	0.5
Q7f	0.38	**<.001**	0.53	0.09	0.07	0.45	0.5
Q8a	**0.004**	**<.001**	0.38	0.13	**0.004**	0.36	**0.03**
Q8b	**<.001**	**<.001**	0.28	**0.005**	**0.002**	0.76	0.12
Q8c	**0.005**	**<.001**	0.07	**<.001**	**<.001**	0.9	0.3
Q8d	0.05	**<.001**	0.24	0.27	**<.001**	0.1	0.07
Q8e	**0.004**	**0.001**	**0.02**	**0.003**	**<.001**	0.56	0.6
Q8f	**0.02**	**0.004**	**0.007**	**0.004**	**0.03**	0.3	0.6
Q8g	0.36	**<.001**	0.38	0.16	**0.02**	0.3	0.3
Q8h	0.1	**<.001**	0.3	**0.02**	**<.001**	0.59	0.5
Q8i	0.6	**<.001**	0.2	0.12	**0.02**	0.2	0.7
Q8j	0.4	**<.001**	0.05	0.9	0.3	0.8	0.7
Q8k	0.3	**<.001**	0.6	0.4	0.06	0.4	0.7
Q9a	**0.006**	0.16	0.16	**0.03**	**0.003**	0.83	0.08
Q9b	**0.001**	0.57	0.34	**0.04**	0.2	0.8	0.3
Q9c	**0.02**	**0.001**	0.43	0.06	**0.01**	0.2	0.1
Q9d	0.2	**<.001**	**0.01**	0.2	**<.001**	0.07	0.8
Q9e	0.37	**<.001**	0.34	0.59	0.13	0.27	**0.04**
Items with signif. eff.	8	20	3	11	16	1	2
Items with marginal eff.	4	0	4	2	2	2	2

Q8b where up to 55.93% reported knowing). For most items, the proportion of respondents who would seek help at some point was consistently highest among those who reported the smallest Internet usage for work or school. The proportion of respondents who would seek help was consistently the highest among those who reported the most minor usage of the Internet for work or school. For specific items (Q7a, Q7c, Q9a, Q8d), the proportion of respondents in the smallest usage group exceeded that of the next group (11-20 hours) by a few percentage points.

Sociodemographic background. Among the employed population, approximately one-third demonstrated proficiency in handling cyber incidents (Q7a, Q7b, Q7c, Q7e), whereas two-thirds expressed a propensity to seek assistance. Moreover, a higher proportion of employed individuals (ranging from 48 to 61%) reported knowledge of solutions for most cyber hygiene items (Q8b, Q8c, Q8e, Q8f). In contrast, this ratio appeared more polarized among students, with up to one-fifth indicating knowledge and four-fifths expressing a willingness to seek assistance. Across all questions, students responded with greater uniformity; however, exceptions were observed. Specifically, slightly over half of the students reported familiarity with setting up multi-factor authentication (Q8b). At the same time, the task of changing home router security settings (Q8h) prompted more than half of the employed population to seek advice.

Age showed statistically significant effect on the cybersecurity hygiene (Q8) and digital privacy questions (Q9) but on none of the incident handling questions (Q7). The general trend was that, compared to other groups, the proportion of respondents reporting knowing a solution is consistently bigger among the 25–34-year-olds. Up to age 34, more respondents knew how to start using a password manager than those who would ask (Q8a). The proportion of individuals who possess knowledge decreases with advancing age. Up to age 54, more respondents knew how to set up multi-factor authentication (Q8b) than those who would ask. The proportion of respondents older than 55 who would ask was more considerable. Among the extreme age groups, the proportion of those needing to ask how to verify the safety of an email (Q8f) or a link (Q8e), or encrypt a file by the receiver's name (Q8c) was greater than those who knew how to do it. The situation was *vice versa* for the rest of the groups (working age), indicating a U-shaped trend. Quite similar U-shaped trends can be observed for Q9a, Q9b, and Q9c, where the proportion of those who would ask was the biggest among the extreme age groups (more than two-thirds). Here, the age group 45-55 stood out for the most minor proportion of people who said they would ask for advice (41.18-47.06%). Among them (compared to other groups), the proportion of those who would do nothing was huge.

Across the three items where **education** significantly influenced responses, the percentage

seeking help ranged consistently from 70.46 to 72.73% among respondents with grammar school education. 20.46 to 29.55% of this group indicated knowledge of the answers. For respondents with higher education, the proportion with knowledge of a solution was consistently higher but never exceeded 41.06%.

Over a half of the respondents who **have cybersecurity caregiver** would seek help when setting up a password manager (Q8a) or limiting inappropriate data collection on their devices (Q9e). Conversely, at least half of those without a cybersecurity caregiver report claim knowledge of how to accomplish these tasks.

Internet usage for other than work/school. The trend for Q7a is evident: with increasing time spent on the Internet for non-work/school purposes, the proportion of respondents who know what to do rises. At the same time, the proportion of those who would ask for help decreases. Interestingly, the only ones who would ignore the problem depicted in this item (social media account hijacked) come from the 41+h group (13.33%).

This analysis suggests that the top third of situations where Estonian home users would seek external advice fall mainly within the domains of cyber situational awareness and incident handling. Additionally, there is interest in learning about setting up and using backup systems for private devices and data. Gender and Internet usage patterns for work/school-related tasks appeared to have a statistically significant effect on the respondents' willingness to seek help in most situations presented to them.

6.3 RQ2: What Characterises the Cybersecurity Support that Estonian Home Users Seek?

To find the priority list of properties of good cybersecurity support in private matters, Q11 asked the respondents: "If you need help with a cybersecurity issue in your private life, what aspects do you think are important in getting such help? Please select the 3 to 4 most important factors." Participants were encouraged to add crucial but missing characteristics into free text field Q12.

The results of Q11 were obtained by counting the ticks that a support characteristic received (Table 8). The distribution of preferences was quite even with no single characteristic was important to more than a fifth of respondents. No characteristic was seen as totally unimportant, although the least prioritised choice was selected by only 1.36% of respondents. The three characteristics of support that were ticked most often were accuracy (17.8%), speed (16.27%) and accessibility (13.9%). Being in the same room with the adviser was

considered the least important aspect of support (1.36%).

Table 8. The priority list of characteristics of informal support as preferred by the survey respondents (n=161). The question (Q11) was, "If you need help with a cybersecurity issue in your private life, what aspects do you think are important in getting such help? Please select the 3 to 4 most important factors." (Options presented in random order.) The characteristics are ranked by the proportion of total count of n=590 single selections made by respondents.

Rank	Characteristic	Ratio
1.	The help is relevant and accurate (accuracy)	17.80%
2.	Help is available quickly (speed)	16.27%
3.	Asking for help is easy (accessibility)	13.90%
4.	The person asking for help understands the explanations given by the person giving help (understandability)	11.69%
5.	The help is for free (cost)	11.36%
6.	The helper relies on official sources (official sources)	7.80%
7.	Help is available regardless of the time of day (time of day)	7.12%
8.	The helper is discreet (discreetness)	6.95%
9.	The person asking for help does not need to explain their situation to the person providing the help, it is familiar to them (no need to explain)	3.22%
10.	The person asking for help does not need to delve into the solution themselves (no need to delve into solution)	2.54%
11.	It is possible to get help in the same room as the provider (location)	1.36%

In free text responses to Q12, two respondents emphasised the trustworthiness of the support giver. One of them backed it with an argument that the accuracy of the support is difficult to assess. Other responses mentioned a trusting relationship, the ability to validate the authenticity of the adviser, avoiding victim blaming, the proactivity of the adviser, and that the supporter was on the side of the support receiver.

6.3.1 RQ5: How Do Preferences for Cybersecurity-related Support Depend on Sociodemographic Variables or Internet Usage?

The author wondered whether the characteristics of desired support would differ for participants of different genders, Internet usage patterns for work or studies-related tasks and those with a cybersecurity caregiver compared to those who lack one. Figure 2 illustrates the preferences of male respondents for cybersecurity support in private matters compared to female respondents. The top five characteristics remain consistent between genders, albeit with variations in their prioritisation, and all characteristics hold significance for at least some respondents. In Figure 3, it can be observed that the priority order remains consistent regardless of whether an individual extensively or rarely uses the Internet for work-related purposes. Similarly, in Figure 4, the lines do not intersect, indicating that

the overall priority order of what is deemed important for cybersecurity support in private matters remains consistent despite having a relationship with a cybersecurity caregiver.

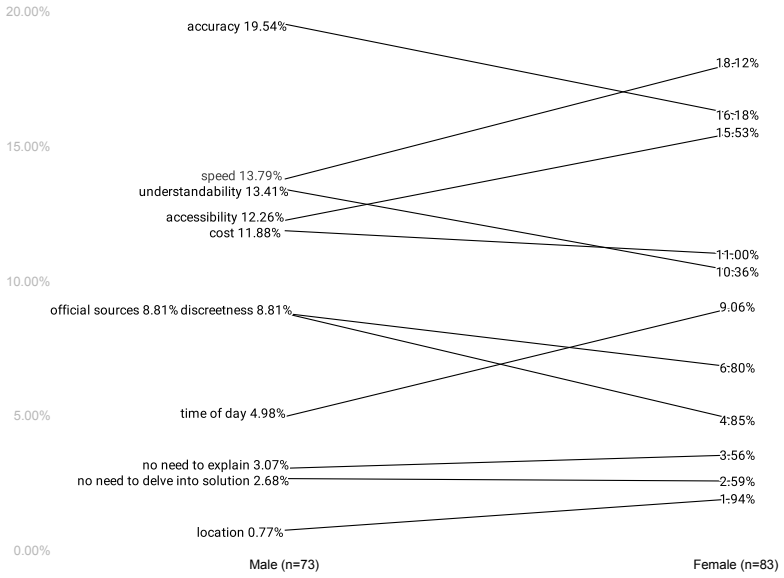

Figure 2. Comparison of the preferred characteristics of cybersecurity support in private matters (Q11) between male (*n*=73) and female (*n*=83) respondents. The characteristics are ranked by the proportion of total count of *n*=572 single selections made by respondents.

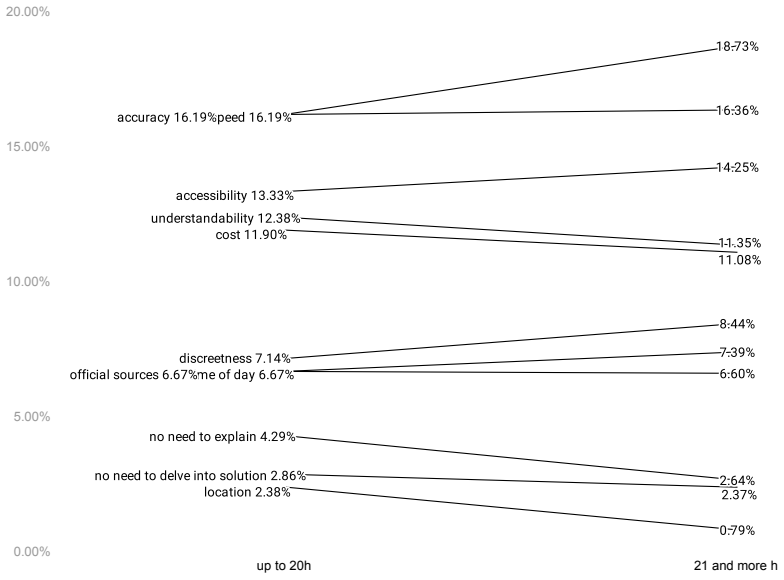

Figure 3. Comparison of preferences for cybersecurity support in private matters (Q11) between respondents who, in a week, spend up to 20 hours in the Internet for work-related task (*n*=58) and those who spend more than 20 hours (*n*=103). The characteristics are ranked by the proportion of total count of *n*=589 single selections made by respondents.

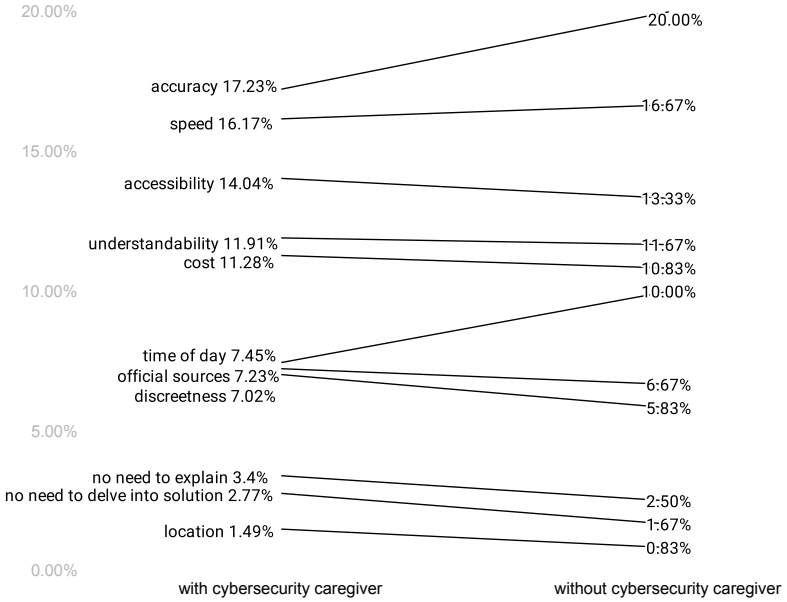

Figure 4. Comparison of preferences for cybersecurity-related support in private matters (Q11) between respondents with (n=129) and without (n=32) cybersecurity caregiver. The characteristics are ranked by the proportion of total count of n=590 single selections made by respondents.

In conclusion, the top five most important characteristics of cybersecurity support, in order of preference, were accuracy, speed, accessibility, understandability, and cost. This ranking remains consistent across different genders and patterns of Internet usage for work/school-related tasks, as well as for individuals with and without cybersecurity caregivers. However, the priority order may vary among these groups. The trustworthiness of the advisor was added by two respondents as free text.

6.4 RQ3: How Different Is the Cybersecurity Support Estonian Home Users Receive from Their Cybersecurity Caregivers from the Support They Seek?

To answer RQ3, the respondents were first asked to choose 3 to 4 (out of 11) aspects of their current support they value the most (Q15). The aspects provided were rephrased from answer options for Q11 that were used for answering RQ2 (see Table 9 for mapping the respective answer options). The results of Q11 (desired characteristics of support) would be compared with the outcome of Q15 (most valued characteristics of current support). Second, one's reality would be observed diverging from the desired state when their assessment of the sufficiency of their current support is negative (Q17). Another indication of insufficiency would be avoidance of contacting one's cybersecurity caregiver

(Q18). Reasons for this avoidance can arise from the source of support, the person asking for support, or something third (Q19, Q20). Only reasons that (are perceived to) arise from the cybersecurity caregiver contribute to answering the research question. Responses from the people with cybersecurity caregiver (n=129) were used for answering RQ3.

The comparison of responses to Q11 and Q15 is depicted in Figure 5. The eleven characteristics clearly divide into two distinct groups, with the top 5 easily identifiable. The most valued characteristics – accuracy, speed, accessibility, understandability, and cost – also define the support that respondents experience. The lines for accuracy and speed cross others, meaning that, although highly desired, the advice of cybersecurity caregivers is not always competent or promptly received.

The findings for RQ2 showed that neither gender, the Internet usage pattern for work, nor the presence of a cybersecurity caregiver alters the composition of the top 5 desired characteristics. Combining this with the current finding of RQ3 leads to infer that these variables do not impose a statistically significant effect also on the results of RQ3.

Table 9. Mapping between answer options of Q11, Q15, and labels used in figures.

Desired characteristic (Q11)	Label	Actual characteristic (Q15)
The help is relevant and accurate	accuracy	The help they give is relevant and accurate
Help is available quickly	speed	They provide help quickly
Asking for help is easy	accessibility	It is easy to ask them
The person asking for help understands the explanations given by the person giving help	understandability	I understand their explanations
The help is for free	cost	Their advice and help are for free
The helper relies on official sources	official sources	They rely on official sources when helping
Help is available regardless of the time of day	time of day	I can ask for help regardless of the time of day
The helper is discreet	discreetness	They are discreet
The person asking for help does not need to explain their situation to the person providing the help, it is familiar to them	no need to explain	I don't need to explain my situation to them, they are familiar with it
The person asking for help does not need to delve into the solution themselves	no need to delve into solution	I don't need to delve into the solution myself
It is possible to get help in the same room as the provider	location	I can get help in the same room with them

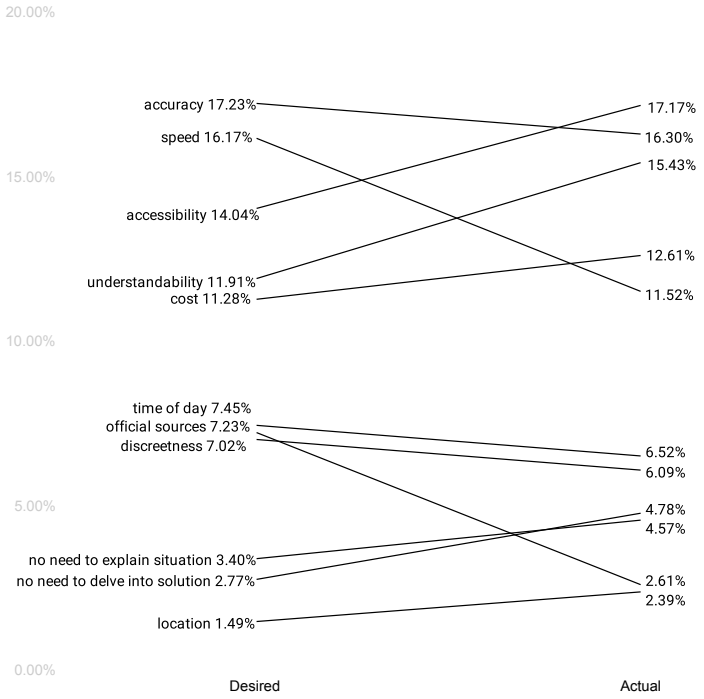

Figure 5. Comparison of the desired characteristics of cybersecurity-related support in private matters (Q11) and the characteristics of actual support (Q15) among respondents who have cybersecurity caregiver (n=129). The characteristics are ranked by the proportion of the total count of single selections, which was n=470 for desired characteristics and n=460 for actual characteristics.

As a desired property of support, again, the trustworthiness of the source of it was added to the free text field Q16. Loyalty that characterises the relationship between relatives was valued ("A relative would never desert me, together we will always find the solution").

For respondents having cybersecurity caregiver but representing various sociodemographic backgrounds and Internet usage patterns, the current support was insufficient for 2.48%, while 18.63% were unsure in their assessment (Q17). Almost a third of respondents admitted avoiding contacting their cybersecurity caregiver for help (Q18). Reasons for this reluctance included fear of inconveniencing (21.96%), embarrassment (14.63%), the prediction that the cybersecurity caregiver would not know the solution (4.88%) and lack of time (2.44%) (Q19). These results suggest that a source of support that alleviates such concerns would benefit certain home users.[1]

[1]The prevalent reason for avoiding contacting the cybersecurity caregiver was a decision to find the solution on their own (51.22%) followed by giving up finding the solution (26.83%). These qualities do not arise from support, but rather from the cybersecurity caregivees themselves, and do not thus contribute to answering RQ3 and are hence reported only for integrity.

To summarise, the support that respondents currently receive is characterised by the same five characteristics that they also value most. However, it is evident that the advice of cybersecurity caregivers is not always readily available as desired.

6.5 RQ4: What Problems Characterise the Informal Cybersecurity Support that Estonian Home Users Receive?

By asking for and receiving assistance, a cybersecurity caregivee can place themselves into a vulnerable situation. They might disclose sensitive information or credentials to the helper, give temporarily away control over their device or accept uninformed or even malicious advice. Survey items Q21, Q22, Q23, Q24 were designed to explore such risky situations. Q26 inquires about incidents of coercion or vote secrecy breach at internet voting. These questions were asked only from participants who had cybersecurity caregiver (n=129).

Q21 asked, "Who enters data into the device?" Answers "The helper" or "Both but I cannot see what they are doing" indicate trusting behaviour that can pose a risk depending on the circumstances. The majority of respondents (81%) claimed they either had control over their device or understood what the helper was doing with it. 11% of the respondents lacked understanding of what cybersecurity caregiver was doing with their device, none of them from the youngest age group. Since 8.5% respondents found the question confusing which was the highest percentage of confusion among questions, Q21 might have suffered from confusing wording.

In Q22 and Q23, respondents presented with six risky situations, were asked to indicate which ones have previously occurred and how likely they are to occur in the future. While processing the results, the answer options for Q22 were assigned numeric values: "No, it has not happened" – 1, "Not sure" – 2, "Yes, it has happened" – 3. For Q23, values 1–5 were assigned to the range of answers starting with 1 for "Totally impossible" to 5 for "Totally possible". Thus, higher scores indicate a more frequent occurrence or higher likelihood to occur, whereas lower scores suggest that the proposed situations had not occurred or were unlikely to happen.

The proportion of respondents who reported they had never experienced any of the proposed situations was consistently above 75.97% (Figure 6). Indicating unsecure practices, responses "Not sure" and "Yes, it has happened" to Q22 are particularly interesting in the context of RQ4 and are summarised in Table 10. The situation that occurred most often was the disclosure of one's PIN codes to the helper (Q22d, had happened to 18.61% of

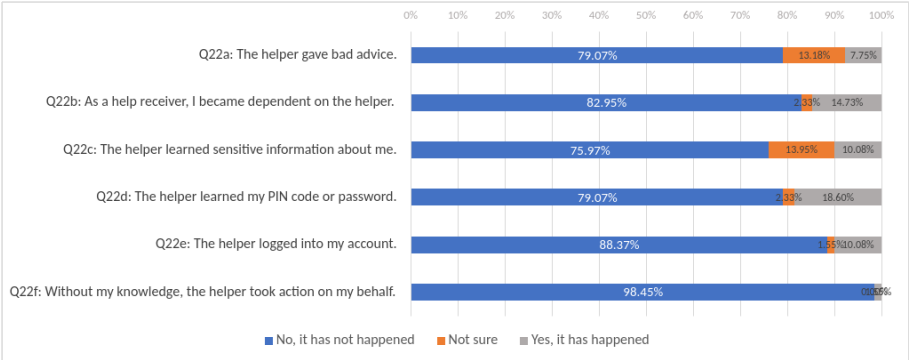

Figure 6. Distribution of results for survey question "Q22. Which of the following situations have happened in your life?" (n=129).

Table 10. Results of the survey question "Q22: Which of the following situations have happened in your life?" The answer options were scored: No, it has not happened – 1, Not sure – 2, Yes, it has happened – 3. n=129.

	Mean Score	SEM	Not sure	Yes, it has happened
Q22a: The helper gave bad advice.	1.29	0.05	13.18%	7.75%
Q22b: As a help receiver, I became dependent on the helper.	1.31	0.06	2.33%	14.73%
Q22c: The helper learned sensitive information about me.	1.34	0.06	13.95%	10.08%
Q22d: The helper learned my PIN code or password.	1.4	0.07	2.33%	18.61%
Q22e: The helper logged into my account.	1.22	0.05	1.55%	10.08%
Q22f: Without my knowledge, the helper took action on my behalf.	1.03	0.02	0.0%	1.55%

respondents and received the highest means score of 1.4). 14.73% of respondents admitted they had experienced becoming dependent on the helper (Q22b, mean score 1.31). For both items Q22c ("The helper learned sensitive information about me.") and Q22e ("The helper logged into my account."), the proportion of "Yes, has happened" responses was 10.08%. Among these, the former received a higher score since many respondents were uncertain whether the helper learned sensitive information about them. The higher percentages of "Not sure" for Q22a and Q22c (13.18 and 13.95%, respectively) indicate respondents' difficulties in assessing the quality of advice and challenges to discern whether the helper learned sensitive information about them. Nearly all respondents were sure that the cybersecurity caregiver never took advantage of their trust by secretly acting on their behalf (Q22f, mean score 1.03).

As for possible misuses of trust in the future (Q23), the chance that the cybersecurity

caregiver would learn sensitive information about the cybersecurity caregivee was assessed as most likely to happen (mean score 3.08) (Table 11). This scenario was followed by the prospect of receiving bad advice (mean score 2.98). Taking secret action on behalf of the cybersecurity caregivee was seen as the least likely (mean score 1.86). Figure 7 provides the overall results for Q23, and Table 11 summarises the results for responses that are most relevant for answering RQ4 – "Somewhat possible" and "Totally possible". Free text field Q24 did not provide any new risky situations. Of the 137 respondents who had i-voted, 8.8% said they have been assisted at this, 3 (2.2%) reported the secrecy of their vote had been challenged, and 2 respondents (1.5%) admitted experiencing coercion. One person said they did not understand the question about coercion.

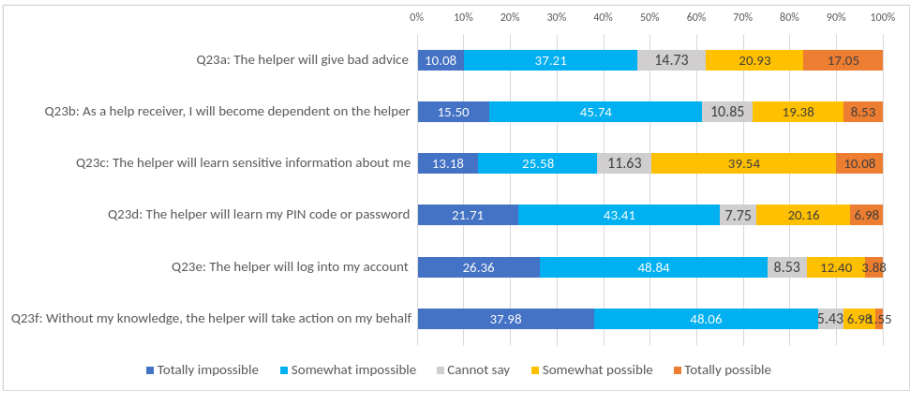

Figure 7. Distribution of results (%) for the survey question "Q23: How likely do you think the following situations are to occur in your life in the future?" n=129.

Table 11. Results of the survey question "Q23. How likely do you think the following situations are to occur in your life in the future?" The answer options were scored: Totally impossible – 1; Somewhat impossible – 2; Cannot say – 3; Somewhat possible – 4; Totally possible – 5. n=129.

	Mean Score	SEM	Somewhat possible	Totally possible
Q23a: The helper will give bad advice.	2.98	0.11	20.93%	17.05%
Q23b: As a help receiver, I will become dependent on the helper.	2.60	0.11	19.38%	8.53%
Q23c: The helper will learn sensitive information about me.	3.08	0.11	39.54%	10.08%
Q23d: The helper will learn my PIN code or password.	2.47	0.11	20.16%	6.98%
Q23e: The helper will log into my account.	2.19	0.10	12.40%	3.87%
Q23f: Without my knowledge, the helper will take action on my behalf.	1.86	0.08	6.98%	1.55%

6.5.1 RQ5: How Do Sociodemographic Variables or Internet Usage Affect the Occurrence of Problems with Informal Support Received by Estonian Home Users?

To answer RQ5, first, an analysis of variance (ANOVA) was conducted to determine which groups exhibit greater variability in scores between them compared to within each group [84, p. 249]. With the post-hoc Tukey test, the groups that exhibit significant differences were discerned. Subsequently, these findings are presented.

Item	Age	Gender	Education	Socioeconomic backgrnd	Internet for work	Internet for other than work
Q22a: The helper gave bad advice.	**0.021**	**<.001**	0.13	0.9	**0.004**	**0.03**
Q22b: As a help receiver, I became dependent on the helper.	0.4	**0.03**	0.5	0.09	0.4	0.5
Q22c: The helper learned sensitive information about me.	0.7	0.7	0.6	0.06	0.7	0.7
Q22d: The helper learned my PIN code or password.	**0.003**	0.4	**0.02**	**<.001**	0.4	0.3
Q22e: The helper logged into my account.	0.7	0.13	0.2	0.1	0.9	0.6
Q22f: Without my knowledge, the helper took action on my behalf.	0.16	0.1	0.7	0.8	0.3	0.5
Q23a: The helper will give bad advice.	**<.001**	**<.001**	0.08	**0.004**	**0.02**	0.5
Q23b: As a help receiver, I will become dependent on the helper.	0.6	0.3	0.3	0.2	0.3	0.5
Q23c: The helper will learn sensitive information about me.	0.7	0.7	0.2	0.6	0.2	0.1
Q23d: The helper will learn my PIN code or password.	**0.02**	0.3	**0.04**	**0.03**	0.2	0.5
Q23e: The helper will log into my account.	0.3	**0.03**	**0.007**	0.2	0.2	0.2
Q23f: Without my knowledge, the helper will take action on my behalf.	0.2	**<.001**	**0.03**	0.2	0.8	0.5

Table 12. ANOVA p-values showing the significance of the effects of socioeconomic variables and Internet usage on the distribution of responses to Q22 and Q23 (n=129). Bold indicates a statistically significant effect (p<0.05).

As summarised in Table 12, responses to the item pair Q22a-Q23a were statistically significantly influenced by most variables (age, gender, both Internet usage variables). Three variables (age, education and Internet usage for work/school) had statistically significant effect on the distribution of responses for item pair Q22a-Q23a. Gender, age

and education were the most influential variables, exposing statistically significant effects on at least three items.

For Q22a, gender had a statistically significant effect [F(1, 124)=16.17, p<0.001]. Post-hoc tests revealed that, compared to women, significantly more men report they received bad advice (mean=1.10, 1.51, respectively).

Also, age had a significant effect [F(5,123)=2.78, p=0.02] on the distribution of responses for this item. Post-hoc tests revealed that the difference is significant between the youngest and the eldest age groups: while the eldest were always content with the advice received, it was not the case with the youngest (mean=1.00 for the eldest, 1.62 for the youngest).

Finally, both Internet usage variables had a significant effect on Q22a [F(3,125)=4.61, p=0.004 for Internet usage for work/studies related tasks, F(3,125)=2.98, p=0.03 for Internet usage for other functions than work/studies]. Post-hoc tests revealed that respondents who used the Internet for work/studies-related tasks more than 41 hours a week were more critical about the informal assistance received. They differ statistically significantly from those who use 0-10h and 21-40h (mean=1.59 for 41+h group, 1.07 for 0–10h group, 1.23 for 21–40h group). Similarly, participants who reported spending more than 41+h on the Internet for tasks other than work/school were more critical about advice received, and their difference from those who spent 0–10h was statistically significant (mean=1.75 for 41+h group, 1.16 for 0–10h group).

Gender had a significant effect on Q22b [F(1,124)=5.02, p=0.03]. The post-hoc test revealed that significantly more women admit that, as help receivers, they have become dependent on help givers (mean=1.16, 1.45, respectively).

For Q22d, socioeconomic status had significant effect [F(3,125)=8.50, p<.001]. Post-hoc tests showed that revealing one's PIN codes is rare among the employed, whereas the practice was more common among the retired and students (mean=1.22 for the employed, 2.22 for the retired, 1.89 for the students).

Also age had significant effect for Q22d [F(5,123)=3.86, p=0.003]. Post-hoc tests showed that, compared to 45–54 year-olds, the proportion of the eldest who had disclosed their PIN codes was significantly bigger (mean=2.00 for 65+, 1.21 for 45–54-year-olds).

For Q22d, also education had statistically significant effect [F(2,126)=4.32, p<.02]. Post-hoc tests revealed a third of respondents with grammar school education reported that they had disclosed their PIN codes to the helper, while the same holds only for 12.22% of

participants with higher education.

Next, the assessment of the likelihood of the six situations happening in the future (Q23) was observed. For Q23a, gender had statistically significant effect [F(1,124)=12,32, p<.001]. Post-hoc test revealed that, compared to women, significantly more men see receiving bad advice more likely (mean=2.62, 3.4 respectively).

As of age, respondents older than 65 years stand out (Q23a). They believe that bad advice is unlikely, and this attitude is statistically significantly different from what three younger age groups think [F(5,123)=5.27, p<.001, mean=3.62 for age group 18–24, 3.21 for 25–34, 3.31 for 35–44, 1.73 for 65+]. There is also a difference between the very young and 55–64-year-olds (mean=2.43 for 55–64-year olds).

The statistically significant effect of socioeconomic background on Q23a reflects the impact of age on these items. Being significantly different from other socioeconomic groups, the retired deny the possibility of receiving bad advice from their caregiver (Q23a) [F(3,125)=4.73, p=0.004, mean=3.64 for others, 3.44 for students, 2.92 for the employed, 1.78 for the retired].

For Q23a, Internet usage for work/school had a significant effect [F(3,125)=3.53, p=0.02]. Post-hoc tests revealed that respondents who work/study 41 or more hours using the Internet, consider receiving bad advice in the future, compared to those who use the Internet for work the least (mean=3.53 for 41+h, 2.52 for 0–10h).

Age had significant effect for Q23d [F(5,123)=2.70, p=0.02]. Post-hoc tests revealed that the oldest age group sees revealing their PIN codes to their cybersecurity caregiver (Q23d) significantly more likely than 45–54 and 55–64-year-olds (mean=3.55 for 65+, 2.14 for 55–64, 2.12 for 45–54).

The statistically significant effect of socioeconomic background reflects the impact of age on Q23d. Compared to the employed, the retired see it significantly more likely that their cybersecurity caregiver would learn their PIN codes (Q23d, F(3,125)=3.03, p=0.03, mean=3.44 for the retired, 2.30 for the employed).

For 23e, gender had a statistically significant effect [F(1,124)=4.70, p=0.03]. Post-hoc test revealed that, compared to women, men are more suspicious about their helper logging on to their account (mean=2.40, 1.98, respectively).

For 23f, gender had a statistically significant effect [F(1,124)=12.40, p<.001]. Post-hoc test

revealed that men see their helper significantly more likely to act on their behalf without them knowing about it (mean=2.16, 1.60, respectively).

Education had a statistically significant effect on the results of three items: Q23d [$F(2,126)=3.45$, $p=0.04$], Q23e [$F(2,126)=5.12$, $p=0.007$] and Q23f [$F(2,126)=3.53$, $p=0.03$]. Post-hoc tests revealed that, compared to respondents with higher education, the ones with grammar school education considered these situations more likely. The respective means were 2.91, 2.29 (Q23d); 2.68, 2.00 (Q22e); 2.19, 1.72 (Q23f).

In conclusion, the survey findings demonstrate that, while the majority of respondents reported never experiencing any of the proposed situations and maintaining control over their devices, some participants engage in unsecure practices. A tenth of survey participants used to give full control over their device to the cybersecurity caregiver. These individuals represented diverse sociodemographic groups, although none were from the youngest age group or from the segment using the Internet for work for more than 41 hours a week. During cybersecurity caregiving sessions, most common risky situations were disclosing one's PIN codes and becoming dependent on the helper. As most likely negative scenarios in the future, participants foresaw the cybersecurity caregiver learning sensitive information about them or giving bad advice.

Different sociodemographic groups evaluated the obtained assistance with varying degrees of criticism. Significantly more men, the young and extensive Internet users reported having received bad advice, compared to their counterparts in other groups. Revealing one's PIN codes was common among students, the eldest age group and respondents with grammar school education, but rare among the employed, the 45–54-year-olds and respondents with higher education. Most these sociodemographic groups project their past experiences into the future. Becoming dependent on the helper had happened to significantly more women than men. Women and participants with grammar school education showed less suspicion about their caregiver logging on to their account or taking action on their behalf without their knowledge.

7. Discussion

To facilitate intervention planning, the current research explores the needs of Estonian home users for cybersecurity assistance and the problems incurred by existing informal support. By examining variations across different socioeconomic groups and among individuals with diverse Internet usage patterns, the study points to areas of improvement and yields practical implications.

Some findings hint that a significant proportion of the survey respondents may have been cybersecurity experts. A consistent 18-29% of respondents claimed knowing how to behave in most of the situations of Q7–Q9. Furthermore, approximately 9% respondents reported advanced knowledge in detecting device compromise. These were tasks that induced a willingness among all other survey participants to seek help. In retrospect, considering that throughout the research period, the author experienced that the term *cybersecurity* deterred less advanced users and excited interest in people familiar with this field. Using alternative wording, such as *Internet usage* in the survey invitation, might have encouraged more laypeople to participate.

7.1 Cybersecurity-related Situations Where Estonian Home Users Would Ask For External Help (RQ1)

According to the current findings, the domains where most home users would reach out for help are cybersecurity situational awareness and handling cyber incidents. Specifically, the items asked under these domains included detecting device compromise or engagement in a cyber attack, monitoring home router traffic, recovering from a ransomware attack or email account takeover, and reporting cybercrime. Indeed, assisting in restoring email and social media accounts emerged as a common task described by the interviewees, who also said they usually report cyber incidents to their cybersecurity caregivees. In an earlier study, adjusting and explaining the security settings of devices was one of the main tasks of tech caregivers [34]. In the present study, understanding the security settings of one's device was an issue that ranked only 17th out of 22 items proposed. At first glance, this suggests that participants may not have perceived it as highly important. Nonetheless, more than half of them (58%) demonstrated readiness to seek help in this regard.

Some of the interviewees said that before recommending solutions and practices to the cybersecurity caregivee, they undergo the analysis of the cybersecurity requirements (e.g.,

the CIA triad) with them. Almost everybody is able to decide their preferences regarding confidentiality, integrity, availability or other security properties and formulate the most terrible scenarios. Based on these findings, it can be proposed that awareness programs that educate citizens to distinguish between security properties would teach them to choose countermeasures to mitigate risks on these properties and verbalise precise questions to ask their helpers. This would spare the cybersecurity caregivers from doing this analysis with them and make tailored advice more likely.

Although a critical and cost-effective measure for better cyber resilience, the questionnaire developed in this study did not address backups. Yet, participants of both phases of the study stated that setting up a backup system for private devices and data is a situation where one may need help. True, choosing a method and software for regular backups and setting it up for personal devices and data is not a straightforward task, nor is restoring from backups upon an incident. It presents its own challenges, involving an understanding of backup systems and the ability to troubleshoot in case of unexpected issues. Advancements in usability have made the process more accessible to home users; for instance, the popular commercial operating systems enable backing up to their clouds. However, it still requires attention to detail and careful management to ensure data integrity and security. Additionally, there is data that individuals cannot afford to lose or disclose, as their or their relatives' well-being depends heavily on this data and options for risk transfer or acceptance are not viable. Based on these considerations and the qualitative data gathered the author proposes that home users should be taught how to choose, configure and use a backup system wisely.

Contradictory findings regarding password management were encountered. Strong and unique passwords are a main way to prevent cybercriminals and malicious software off from one's devices and accounts. The interviewees expressed the importance of credential management, with one of them highlighting that widespread adoption of it could significantly improve the cybersecurity posture of the whole society. According to them, a password manager can also serve as an asset inventory for one's accounts, as a good overview of one's assets is a prerequisite for successful cybersecurity management. Aspects of credential management were often the focus of cybersecurity caregiving sessions described in all interviews. Specifically, discussions (initiated by both, cybersecurity caregivee or caregiver) about strong passwords, passphrases and keys were frequent, as well as selecting a suitable password manager for the caregivee. Multi-factor authentication was often set up for the first time during the caregivee's account restoration. Therefore, the majority of the survey participants were expected to express a need for assistance in starting using a password manager or setting up MFA. Instead, as much as approximately half of them claimed they already possessed knowledge of these tasks, ranking these as

the last ones among the 22 items asked. It is possible that the skew in the sample towards employed participants with higher education influenced these findings: the stricter security policies of employers in the technology sector could potentially drive the adoption of this countermeasure.

Alternatively, the current findings regarding password managers may be an indication of the phenomenon described in [30], [28]. Specifically, people report knowledge of cybersecurity practices (as also shown by the current survey results) but are reluctant to implement these in practice (as suggested by the interviews). Furthermore, [49] describes that while exposure to personally relevant data breaches increased participants' *willingness* to improve their online behaviour, no change in their *actual* practices was observed. If this is the case, it is worth highlighting research [66] that shows that the availability of situational support can change individuals' cybersecurity practices for the better. They claim that by raising one's belief that one will succeed, the availability of adequate support increases one's self-efficacy. In numerous studies, the latter concept has been shown as a predicting factor for adopting cyber-aware behaviours [65], [64], [67], [68]. Therefore, guaranteeing access to cybersecurity support for everyone could have a positive influence on their self-efficacy and the likelihood of adopting cybersecurity best practices.

The National Cyber Security Centre of Estonia promotes using a password manager but cautions about the need for careful evaluation of specific applications due to past breaches [60]. While this is a valid recommendation, it must be accepted that many home users may lack the expertise to perform this assessment. Also one of the interviewees pointed out that the steep learning curve prevents many people from adopting it. One can see a need for education on password managers, including their functionality, differences, setup process, and best practices for use in everyday life as well as upon an incident like account hijacking.

Besides the ability to manage one's credentials, another skill critical for being safe online is distinguishing between safe, suspicious and malicious links. Although more than a third of the survey respondents were aware of how to verify the safety of a link, an interesting behaviour among another group was observed. Remarkably, 16% of respondents, despite reading the recommendations about checking the safety of links provided in the survey, still claimed they were unable to do so. Given that diagnosing links for their caregivees was a common task reported by the interviewees, checking links may be perceived as too difficult by some individuals, leading them to either rely on others' expertise or ignore the necessity overall.

It should be acknowledged that some citizen groups will never adopt new cybersecu-

rity countermeasures on their own and will remain relying on their cybersecurity caregivers for several technical tasks. In the absence of a cyber caregiver, they may overlook cybersecurity-related matters altogether. The phenomenon of tech caregiving, including cybersecurity caregiving, exists and will remain in Estonian society and can be relied upon to enhance the population's cyber resilience. Empowering cybersecurity caregivers by addressing awareness campaigns to them [28], [34], would make them aware of their role and accompanying responsibility as well as ways how to enhance the cyber hygiene of their caregivees proactively. According to the interviews of this study and [34], cybersecurity caregivers tend to find answers to questions by googling. Therefore, they are the segment that would digest the information provided online (FAQ pages, checklists, topics to talk to with their caregivees, information about how local e-services work, the parties operating in the society like common marketplaces, and courier companies). A cybersecurity expert interviewee demonstrated thorough acquaintance with the contents of national cybersecurity awareness campaigns such as Be IT-conscious [23] suggesting that such online content is attractive to cybersecurity professionals. Thankfully, this awareness campaign encourages knowledge sharing among individuals by ending videos with a call: "Tell also your neighbour..."[1] Maybe such campaigns should be more openly addressed to cybersecurity caregivers and not only to laypeople?

7.2 Characteristics of Cybersecurity-related Support Important to Estonian Home Users (RQ2), Compared To the Informal Support They Currently Receive (RQ3)

From the eleven characteristics provided, the respondents showed a desire for cybersecurity advice that is accurate, prompt, easy to seek and understand, and free of charge. Interestingly, the same characteristics remain consistent across the sociodemographic variables that influenced most RQ1 items: gender and Internet usage for work. Moreover, these properties characterise also the actual support received, albeit in a different priority order. Notably, the actual support is not always promptly available. Also, for instance, 8% of the survey respondents had experienced bad advice and 13% were unable to assess the quality of help received. Similarities between the results of the current study and the findings of [28] can be observed. In their endeavour to understand how a source of support is chosen, perceived competence was desired by the vast majority of their study participants. For a third of their respondents, trusting relationships, cost, and constant availability (speed) were considered important factors when selecting a source of support. However, the results of the current work diverge from one of their findings. In case something went wrong, their participants expressed a wish to be able to return to the same person. On the contrary,

[1]For example, the video at https://www.itvaatlik.ee/kaitse/. Accessed 29.04.2024.

Estonian home users did not rank the respective item pair – "The person asking for help does not need to explain their situation to the person providing the help, it is familiar to them." and "I don't need to explain my situation to them, they are familiar with it." – high at all.

Some interviews in the current study unveiled a principle of effective support that deserves highlighting, although it was not addressed in the survey. Cybersecurity support should be tailored to the cybersecurity needs for confidentiality, integrity, and availability of the recipient rather than the preferences of the helper. An adviser can explain why they recommend particular countermeasures, but should not assume that their own preferences hold for the caregivee.

7.3 Problems that Occur with the Current Informal Cybersecurity Support

Almost a fifth of the survey respondents admitted having revealed their PIN codes, and 15% confessed dependency on the cybersecurity caregiver. Other situations had occurred less often, with the most serious one – taking secret action on behalf of the caregivee – being experienced by a few. Particularly hard were assessing the quality of advice and knowing whether one had revealed sensitive information to the helper (13% of participants responded "Not sure"). Also, [28] argues that, for a home user, evaluating the quality of advice and differentiating between a competent individual and an incompetent or malicious one is a challenge.

For all six proposed situations, a consistent majority of respondents declared never experiencing these. This is an encouraging finding, provided it accurately reflects the reality. Instead of documenting incidents, these self-reported results may rather hint at whether the respondents have been able to recognise these scenarios in their lives. Informing laypeople about the risks associated with informal cybersecurity support could potentially reduce the occurrence of such situations. However, it must be approached with caution to avoid harming trusting relationships essential for the connectedness and strength of society.

To reduce dependency on the helper, some interviewees described guiding their cybersecurity caregivees to become more self-reliant. They do this by suggesting keywords for googling, instructing them to apply solutions themselves, and avoiding touching the caregivee's device. Nevertheless, a tenth of the respondents from various sociodemographic groups were giving full control over their devices to the cybersecurity caregiver.

7.4 The Influence of Sociodemographic Variables and Internet Usage on Respondents' Cybersecurity Preparedness (RQ5)

The interviewees of the current research reported assisting friends and relatives of both genders and all age groups. They also emphasised that even people who use the Internet minimally for their work express concerns about securing their devices, and those using the Internet for work extensively can practice unsecure activities like impulsive clicking. Therefore, various socioeconomic groups were expected to respond to the survey questions similarly. Indeed, their understanding of what is important at cybersecurity related support were quite uniform (RQ2), as were their experiences with the support they currently receive from their cybersecurity caregivers (RQ3). However, gender, age, education, socioeconomic background, and the amount of Internet used for work significantly influenced their willingness to seek cybersecurity-related support (RQ1), as well as support-related problems experienced and anticipated (RQ4). For example, for all cybersecurity incident handling, cybersecurity hygiene and cyber situational awareness questions, constantly more men than women reported knowledge of a solution. This witnessed difference in self-perception between men and women aligns with results of prior work [85] where gender had a significant effect on self-reported cybersecurity behaviours. Analysing the data of 27,000 Europeans, [86] argues that "women do not necessarily demonstrate a lower level of cybersecurity preparedness than men."

The influence of age was not linear in the current findings, rather it took a U-shaped form. It was similar to the results of [87] where the younger and older Internet users appeared less protective of their privacy, compared to middle-aged individuals. In the sample of this work, a higher level of familiarity with cyber hygiene among age groups predominantly composed of working individuals was observed, as opposed to students. The effect of socioeconomic background (employment) mirrored the effect of age. The exceptions that emerged here – adopting password manager or setting up MFA were well known by the young – hint that cybersecurity knowledge and needs vary across cybersecurity situations [68]. In the current research, the survey corroborated the observation made by an interviewee that the young have not yet developed substantial experience to differentiate between normal and suspicious emails.

The effect of Internet usage for work/school-related tasks showed a clear effect on all cyber hygiene items and on most incident handling, cyber awareness and privacy questions. The bigger the proportion of extensive Internet users for work/school-related tasks, the bigger the proportion reporting knowing a solution. And *vice versa* – the smaller the proportion of respondents using the Internet for work/school-related tasks, the bigger the

amount would reach out for help. Similarly, [88] confirmed that the more frequent one's Internet use was, the more they reported willingness to engage in cyber-safety behaviour. However, one should not rush to the conclusion that spending many hours online makes one knowledgeable in most cybersecurity questions. Instead, the possibility of witnessing the overconfidence observed among the more IT-savvy individuals earlier [89] should be considered. In their research, individuals with a background in information technology – contrary to their own expectations – did not perform superior in judging the authenticity of deep fakes, compared to other participants.

Even without differentiating between employment in information technology or other sectors, a consistently larger proportion of the employed respondents reported knowledge of cyber hygiene and incident handling compared to students and the elderly. Combining this finding with the influences of age, Internet usage patterns, and education, one can conclude that better cyber security preparedness is reported among higher-educated, middle-aged, and employed population with jobs involving profound Internet usage. This outcome may be attributed to cyber training organised by employers whose employees extend the usage of knowledge obtained at work for use in private matters. For instance, the task of changing home router security settings – likely not covered in cybersecurity programs at work – prompted more than half of the employed respondents to seek advice. It can only called an "outcome" and not the success since still at least half of the employed would seek help for most items, highlighting their need for the availability of cybersecurity support in private matters. Other groups – the unemployed, housewives and -husbands, students and the retired – can be considered even less prepared for safely acting in cyberspace, thus urgently needing special attention by those responsible for the population's cybersecurity preparedness.

7.5 Summarising Practical Implications

Equitable access to cybersecurity support should be available to all citizens despite their sociodemographic background or Internet usage pattern. The current findings give ground to subjectively suggest that individuals without cybersecurity training provided at work are less prepared to manage their devices, data and accounts and to handle cyber incidents. They need trustworthy support from elsewhere. Friends and family can provide this but relying on informal support presupposes the ability to recognise risks: unintentional or intentional bad advice, dependency on another individual, disclosure of sensitive information or credentials, and misuse of trust.

According to the current results, desired support is accurate, prompt, free of charge, easily understood and accessed by the help seeker as well as adjusted to their cybersecurity

requirements. These criteria can be met by a synchronous communication channel such as a hotline (e.g., web chat and phone) manned with knowledgeable cybersecurity experts obliged to keep confidentiality. Unlike in Estonia, such hotlines are established in, for example, Germany [90], [91] and Spain [92], [93]. Based on the findings of this study, requests for advice about incident handling and cyber situational awareness would be more frequent compared to cyber hygiene and digital privacy.

There is a need to educate the population about personal requirements for cybersecurity (i.e., the CIA triad). Having identified these, one is better prepared to choose appropriate countermeasures (e.g., a backup system or a password manager) and seek advice from any type of support, be it a support channel, another person or a resource in written form. The process of selecting cybersecurity measures could further be facilitated by online resources presented as decision trees prepared by the cybersecurity experts of a trustworthy institution from the academia, public or private institution.

It should be accepted that there are people who will never keep up with the accumulation of cybersecurity countermeasures one has to master and will always rely on someone else. As a phenomenon already existing in society, cybersecurity caregiving is a structure upon which – if done carefully and wisely – nationally organised cybersecurity support can partly rely upon. By educating cybersecurity caregivees to disclose only minimal information and empowering cybersecurity caregivers with resources tailored to them, the latter can be valuable partners to the official agencies responsible for the cybersecurity resiliency of the population.

7.6 Limitations and Future Work

The research faces certain limitations that have to be taken into consideration when pursuing nuanced interpretation. A requirement of a master's thesis foresees the presence of a single author. This may introduce a researcher bias in the interpretation of qualitative data despite approaching them according to an established research plan, in several cycles, and with an open mind. Both methods utilised in the study gathered self-reported data which may have been influenced by factors like wanting to give socially acceptable answers, memory lapses, or misunderstanding questions. This potential for response bias could impact the generalisability of the findings. However, in the current work, qualitative data collection was employed to gain deeper insights into the phenomenon of cybersecurity caregiving and inform the development of the survey instrument. At the same time, the self-reported nature of survey results holds relevance in the study, as respondents' perception determines their actions, and this is what is important. Optimism bias could have influenced respondents' answers to survey questions regarding the likelihood of experiencing misuse of trust by

their cyber caregivers in the future.

A web survey reaches only part of the population. It may miss individuals who do not engage in online activities, contributing to coverage bias. To mitigate this, interviewees were urged to encourage their cybersecurity caregivees to participate, and survey invitations requested recipients to share the survey with relatives of diverse demographics and internet habits. Even though the current findings depict the cybersecurity support needs of individuals who are more active online, it is reasonable to infer that the situation is not substantially more optimistic for those who did not participate in the survey. Segments of the population like the unemployed and housewives/husbands who lack access to institutional cybersecurity support available to many employed individuals, warrant further profound research utilising carefully chosen study instruments.

Similarly, since the research was conducted in Estonian, the insights from the population segments who do not comprehend the language[2] could be the focus of another study. For legal reasons, minors were excluded from the study. However, as extensive users of Internet, devices and accounts, investigating them in the context of cybersecurity caregiving would be a fruitful direction of research, beneficial for any society.

With the increasing adoption of large language models in various aspects of our lives, future research avenues should explore risks of and home users' experiences in utilising these as cybersecurity assistants or caregivers. One interviewee admitted that, for them, a driving force for adopting good cybersecurity practices was what he called a cybersecurity culture: using a password manager or a security token was cool. Investigating aspects of this self-emerging cyber culture would provide insights into which practices and why are rapidly embraced by some segments of the population while disregarded by others.

[2]With Estonian being the only official language in the country, non-Estonian speakers made 16% of the population by the end of 2021, according to the results of the census [94].

8. Summary

The prerequisite of safe engagement in cyberspace is the ability to find help in case unexpected issues with one's devices, accounts or data occur. In the absence of a dedicated cybersecurity-related support service accessible to every Estonian citizen, laypeople seek help from their friends and family when in need to diagnose and solve a cybersecurity problem. This explorative mixed methods study investigated the needs of Estonian home users for cybersecurity-related support for private (that is, not work-related) matters and experiences of trust misuse or other risky situations incurred by their current informal support. The concept of tech caregiving was employed where individuals voluntarily assist others without compensation, narrowing the focus further to the cybersecurity field and coining a new term *cybersecurity caregiving*. Through seven interviews with cybersecurity caregivers, insights to develop a survey targeting the adult population of Estonia were gained. The survey asked in which of the proposed situations the respondents would seek help, report existing knowledge of solutions, or, instead, do nothing. It also explored how different is their desired support from what they currently receive from their cybersecurity caregiver and what risky situations associated with informal support sessions they have undergone.

161 individuals responded to the survey, representing the gender and age distribution of the Estonian population, including a significant proportion of employed individuals and students. For the survey participants, the most important characteristics of cybersecurity support in private matters were accuracy, speed, accessibility, understandability, and cost. The cybersecurity-related support they currently receive from their cybersecurity caregivers was also characterised by these five characteristics, albeit help could be more prompt. Additionally, the current qualitative study pointed out that cybersecurity support should be tailored to the cybersecurity requirements of the help seeker. While the majority of the survey participants reported they had never recognised that receiving help would place them in a vulnerable position, some respondents reported unsecure practices. For proposed cybersecurity-related situations, constantly a higher proportion of respondents expressed willingness to seek assistance and a smaller proportion reported knowing a solution. Therefore these findings propose that support should cover topics of cyber hygiene, incident handling, cyber situational awareness and digital privacy. The influence of sociodemographic background and Internet usage pattern seen in the findings suggest that better cyber security preparedness is reported among higher-educated, middle-aged, and employed population with jobs involving extensive Internet usage. However, still,

at least half of the employed would seek help in most cybersecurity situations proposed to them. Therefore, other population segments – the unemployed, students, the retired, housewives and -husbands – can be considered even less ready to safely utilise their devices, accounts and data. The present findings also hint that there remain people who will never keep up with the changing landscape of cybersecurity countermeasures and will always need someone to assist them. Thankfully, respondents from all population groups exhibited a high level of willingness to seek help in case they do not know a solution to a proposed cybersecurity-related issue in their private lives. Only a marginal amount of participants reported they would do nothing. This encourages a conclusion that the whole population would benefit from educating laypeople to distinguish between and decide their personal cybersecurity requirements, empowering the cybersecurity caregivers with resources tailored to them, and establishing a free-of-charge cybersecurity support service that provided accurate, prompt, easily asked for and understandable advice adjusted to the help seeker's cybersecurity requirements.

To even better facilitate education and intervention planning in Estonia, a similar survey could be conducted among minors and residents who do not speak Estonian. Future research could explore the risks of and home users' expectations in utilising large language models as cybersecurity assistants. Also, investigating aspects of the self-emerging cyber culture would provide an understanding of why some cybersecurity countermeasures are rapidly embraced by some population segments while disregarded by others.

References

[1] *The Digital Economy and Society Index (DESI) 2022. Thematic Chapters*. Publisher: European Commission. Accessed 02.11.2023. 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

[2] *Global Cybersecurity Index 2020. Measuring commitment to cybersecurity. ITU Publications*. Accessed 15.11.2023. 2023. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

[3] *This is the story of the world's most advanced digital society. e-Estonia*. Accessed 05.09.2023. URL: https://e-estonia.com/story/.

[4] Nathan Heller. "Estonia, the Digital Republic". In: *The New Yorker* (Dec. 11, 2017). Accessed 05.09.2023. URL: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

[5] Erdem Suna. ""Right, f*** it. We'll do it ourselves": The sentence that turned Estonia from Soviet backwater to digital miracle". In: *The European* (Jan. 27, 2022). Accessed 05.09.2023. URL: https://www.theneweuropean.co.uk/estonia-and-its-digital-expansion-in-the-full-digital-nation/.

[6] *Estonia – The Digital Nation. Estonian Convention Bureau*. Accessed 05.09.2023. URL: https://www.ecb.ee/blog/venues/estonia-the-digital-nation/.

[7] *Estonia. Digital Nations*. Accessed 05.09.2023. URL: https://www.leadingdigitalgovs.org/estonia.

[8] *Terms of Use. Brand Estonia*. Accessed 05.09.2023. URL: https://brand.estonia.ee/help/terms/?lang=en.

[9] *Estonia as an international cybersecurity leader. e-Estonia*. Accessed 05.09.2023. Aug. 21, 2019. URL: https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/.

[10] *Cyber Security. Factsheet.* Accessed 05.09.2023. URL: https://e-estonia.com/wp-content/uploads/factsheet-cyber-security-feb2023.pdf.

[11] Margus Muld. *Kõik kutselised kalurid peavad hakkama püügipäevikut elektroonselt täitma. ERR*. Accessed 02.11.2023. Oct. 19, 2023. URL: https://www.err.ee/1609138964/koik-kutselised-kalurid-peavad-hakkama-puugipaevikut-elektroonselt-taitma.

[12] *You Are A Target*. Publisher: SANS. Accessed 15.11.2023. 2021. URL: https://www.sans.org/posters/you-are-a-target/.

[13] F. Assolini. *The tale of one thousand andone DSL modems*. Accessed 15.11.2023. 2012. URL: https://securelist.com/the-tale-of-one-thousand-and-one-dsl-modems/57776/.

[14] Brian Krebs. *Lizard Stresser Runs on Hacked Home Routers*. Accessed 15.11.2023. 2015. URL: https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[15] Malwarebytes. *What was the Mirai botnet?* Accessed 28.02.2024. URL: https://www.malwarebytes.com/what-was-the-mirai-botnet.

[16] Brian Krebs. *KrebsOnSecurity Hit With Record DDoS*. Accessed 02.10.2023. 2016. URL: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[17] *Smart home devices used as weapons in website attack*. Accessed 15.11.2023. 2016. URL: http://www.bbc.co.uk/news/technology-37738823.

[18] Lukasz Olejnik and Artur Kurasiński. *Philosophy of Cybersecurity*. CRC Press, 2023.

[19] *Factsheet of The EU's Cybersecurity Strategy for the Digital Decade*. Publisher: European Commission. Accessed 29.04.2024. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

[20] *The EU's Cybersecurity Strategy for the Digital Decade*. Publisher: European Commission. Accessed 09.04.2024. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[21] Betty-Ester Väljaots. *Luukas Ilves: poliitikas osalemine ei peaks tähendama soodsat ametikohta*. Accessed 30.03.2024. 2024. URL: https://www.postimees.ee/7990083/nadala-persoon-luukas-ilves-poliitikas-osalemine-ei-peaks-tahendama-soodsat-ametikohta.

[22] *"Ole valmis!" äpp aitab kriisiolukordadeks valmistuda. Naiskodukaitse*. Accessed 28.02.2024. URL: https://www.naiskodukaitse.ee/OLE%5C_VALMIS%5C_3680.

[23] *Ole IT-vaatlik - Be IT-conscious! Information System Authority*. 14.07.2023. URL: https://www.itvaatlik.ee/en/.

[24] *Report a crime. Police and Border Guard*. Accessed 28.02.2024. URL: https://cyber.politsei.ee/en/.

[25] *VIP Security. Cybers*. Accessed 11.07.2023. URL: https://cybers.eu/en/cyber-defense-center/offensive-security/vip-security.

[26] K. Eensaar. "Ööpäevaringset tervisenõu saab küsida perearsti nõuandetelefonilt 1220". In: (). Accessed 21.03.2024. URL: https://tervis.postimees.ee/3337507/oopaevaringset-tervisenou-saab-kusida-perearsti-nouandetelefonilt-1220.

[27] *Olulised nõuandetelefonid. Patsientide liit*. Accessed 21.03.2024. URL: https://www.patsiendid.ee/partnerid/nouandetelefonid.

[28] Norbert Nthala and Ivan Flechais. "Informal Support Networks: an investigation into Home Data Security Practices". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 63–82. ISBN: 978-1-939133-10-6. URL: https://www.usenix.org/conference/soups2018/presentation/nthala.

[29] Sarah Turner. "Approaches and Technologies to Support Home Users' Engagement with Cyber Security". In: *Proceedings of the 33rd International BCS Human Computer Interaction Conference (BCS HCI 2020)*. 2020. DOI: 10.14236/ewic/HCI20DC.14.

[30] Emma Osborn and Andrew Simpson. "Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study". In: *The Computer Journal* 61.4 (Sept. 2017), pp. 472–495. ISSN: 0010-4620. DOI: 10.1093/comjnl/bxx093. eprint: https://academic.oup.com/comjnl/article-pdf/61/4/472/24509646/bxx093.pdf. URL: https://doi.org/10.1093/comjnl/bxx093.

[31] Thulani Mashiane and Elmarie Kritzinger. "Cybersecurity Behaviour: A Conceptual Taxonomy". In: *Information Security Theory and Practice*. Ed. by Olivier Blazy and Chan Yeob Yeun. Cham: Springer International Publishing, 2019, pp. 147–156. ISBN: 978-3-030-20074-9.

[32] Ying Li, Xin Tong, and Mikko Siponen. "Citizens' Cybersecurity Behavior: Some Major Challenges". In: *IEEE Security & Privacy* PP (Oct. 2021), pp. 2–9. DOI: 10.1109/MSEC.2021.3117371.

[33] Puspadevi Kuppusamy et al. “INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR MODELS, THEORIES, AND INFLUENCING FACTORS: A SYSTEMATIC LITERATURE REVIEW”. In: *Journal of Theoretical and Applied Information Technology* 100.5 (2022). Cited by: 0, pp. 1536–1557.

[34] Jess Kropczynski et al. “Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving”. In: *Proc. ACM Hum.-Comput. Interact.* 5.CSCW2 (Oct. 2021). DOI: 10.1145/3479540. URL: https://doi-org.ezproxy.utlib.ut.ee/10.1145/3479540.

[35] Sanjana Kaushik. *Social Networks of Technology Caregivers and Caregivees*. 2020. URL: http://rave.ohiolink.edu/etdc/view?acc_num=ucin1613749933487134.

[36] *Conversation and correspondence with the leading experts of the Cybersecurity Branch of Estonian Information System Authority (RIA)*. October 2022.

[37] Mahdi Nasrullah Al-Ameen et al. “" We, three brothers have always known everything of each other": A Cross-cultural Study of Sharing Digital Devices and Online Accounts.” In: *Proc. Priv. Enhancing Technol.* 2021.4 (2021), pp. 203–224.

[38] Rohani Rohan et al. “Understanding of Human Factors in Cybersecurity: A Systematic Literature Review”. In: *2021 International Conference on Computational Performance Evaluation, ComPE 2021* (Dec. 2021), pp. 133–140. DOI: 10.1109/ComPE53109.2021.9752358.

[39] *Europe’s Digital Decade: digital targets for 2030*. Accessed 29.04.2024. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

[40] Adam N Joinson et al. “Development of a new ‘human cyber-resilience scale’”. In: *Journal of Cybersecurity* 9.1 (2023), tyad007. DOI: https://doi.org/10.1093/cybsec/tyad007.

[41] Scientific Advice Mechanism High Level Group. *Scientific advice mechanism scoping paper: Cybersecurity*. Accessed 29.04.2024. 2016. URL: https://research-and-innovation.ec.europa.eu/system/files/2020-02/hlg_sam_012016_scoping_paper_cybersecurity.pdf.

[42] Igor Linkov and Alexander Kott. “Fundamental concepts of cyber resilience: Introduction and overview”. In: *Cyber resilience of systems and networks* (2019), pp. 1–25.

[43] Mamello Thinyane and Debora Christine. “SMART Citizen Cyber Resilience (SC2R) Ontology”. In: *13th International Conference on Security of Information and Networks*. 2020, pp. 1–8.

[44] Fredrik Björck et al. “Cyber resilience–fundamentals for a definition”. In: *New Contributions in Information Systems and Technologies: Volume 1*. Springer. 2015, pp. 311–316.

[45] Norbert Nthala and Ivan Flechais. “Rethinking home network security”. In: *European Workshop on Usable Security (EuroUSEC) 2018*. Internet Society. 2018.

[46] Matt Bromiley. “Personal Security with Agency”. White Paper Firstlook. 2023. URL: https://www.sans.org/white-papers/personal-security-with-agency/.

[47] Kjell Hausken. “Cyber resilience in firms, organizations and societies”. In: *Internet of Things* 11 (2020), p. 100204.

[48] Steve M Furnell, Peter Bryant, and Andrew D Phippen. “Assessing the security perceptions of personal Internet users”. In: *Computers & Security* 26.5 (2007), pp. 410–417.

[49] Nadiya Kostyuk and Carly Wayne. “The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public”. In: *Journal of Global Security Studies* 6.2 (2021). Cited by: 17. DOI: 10.1093/jogss/ogz077. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096861524&doi=10.1093%5C%2fjogss%5C%2fogz077%5C&partnerID=40&md5=9e368767888225a0a2bab7400a66a269.

[50] Rob Manwaring and Josh Holloway. “Resilience to cyber-enabled foreign interference: citizen understanding and threat perceptions”. In: *Defence Studies* 0.0 (2022), pp. 1–24. DOI: 10.1080/14702436.2022.2138349. eprint: https://doi.org/10.1080/14702436.2022.2138349. URL: https://doi.org/10.1080/14702436.2022.2138349.

[51] Sarah Turner, Jason Nurse, and Shujun Li. “When Googling It Doesn’t Work: The Challenge of Finding Security Advice for Smart Home Devices”. In: *Human Aspects of Information Security and Assurance*. Ed. by Steven Furnell and Nathan Clarke. Cham: Springer International Publishing, 2021, pp. 115–126. ISBN: 978-3-030-81111-2.

[52] Hasti Sharifi and Debaleena Chattopadhyay. “A Cross-Cultural Study of Relational Maintenance in Tech Caregiving”. In: *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 2023, pp. 1–10.

[53] James Nicholson and Jill McGlasson. “CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support”. In: *Companion Publication of the 2020 ACM Designing Interactive Systems Conference*. DIS’ 20 Companion. Eindhoven, Netherlands: Association for Computing Machinery, 2020, pp. 117–

121. ISBN: 9781450379878. DOI: 10.1145/3393914.3395871. URL: https://doi-org.ezproxy.utlib.ut.ee/10.1145/3393914.3395871.

[54] Matthew Canham et al. “Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards”. In: *SAGE Open* 11 (Feb. 2021), p. 215824402199065. DOI: 10.1177/2158244021990656.

[55] Anneli Heinsoo. *Anneli Heinsoo: digihügieeni parandamisega loome usaldust ka digiriigi vastu*. Accessed 19.09.2023. 2023. URL: https://www.err.ee/1608933068/anneli-heinsoo-digihugieeni-parandamisega-loome-usaldust-ka-digiriigi-vastu.

[56] Käte-Riin Kont. “Balti riikide raamatukotöötajate infoturbeteadlikkus: võrdlev analüüs”. In: *Turvalisuskompass : turvalisuse ja julgeoleku teadusajakiri* 5 (2023), pp. 297–326.

[57] *Tasks and structure of the authority. Information System Authority*. Accessed 12.02.2024. URL: https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority.

[58] *News. Information System Authority*. Accessed 12.02.2024. Filtered by Situation in the cyberspace. URL: https://www.ria.ee/en/search?type=News%5C&sort%5C_by=created.

[59] *Cyber Security in Estonia 2023*. Republic of Estonia State Information Agency, 2023. URL: https://ria.ee/media/2702/download.

[60] Riigi Infosüsteemi Amet. *Petised võtsid Eesti firma meilivestluse üle ja 30 000 eurot oligi läinud. Usutlus RIA küberturbe ekspertidega*. Accessed 25.03.2024. URL: https://digipro.geenius.ee/blogi/turvalise-e-riigi-blogi/petised-votsid-eesti-firma-meilivestluse-ule-ja-30-000-eurot-oligi-lainud/.

[61] Statistics Estonia. *Infotehnoloogia leibkonnas 2022. aasta*. Accessed 29.04.2024. URL: https://www.stat.ee/sites/default/files/2022-03/ITL2022_paberankeet_EE.pdf.

[62] Statistics Estonia. *IT46: KNOWLEDGE OF INTERNET COOKIES AND THEIR LIMITATION IN BROWSER AMONG 16–74 YEAR OLD INTERNET USERS BY GROUP OF INDIVIDUALS*. Accessed 29.04.2024. URL: https://andmed.stat.ee/en/stat/majandus__infotehnoloogia__infotehnoloogia-leibkonnas/IT46.

[63] Norbert Nthala and Ivan Flechais. ""If It's Urgent or It Is Stopping Me from Doing Something, Then I Might Just Go Straight at It": A Study into Home Data Security Decisions". In: *Human Aspects of Information Security, Privacy and Trust*. Ed. by Theo Tryfonas. Cham: Springer International Publishing, 2017, pp. 123–142. ISBN: 978-3-319-58460-7.

[64] Thulani Mashiane and Elmarie Kritzinger. "IDENTIFYING BEHAVIORAL CONSTRUCTS IN RELATION TO USER CYBERSECURITY BEHAVIOR". In: *EURASIAN JOURNAL OF SOCIAL SCIENCES* 9 (Jan. 2021), pp. 98–122. DOI: 10.15604/ejss.2021.09.02.004.

[65] Sumesh J. Philip, Truong (Jack) Luu, and Traci Carte. "There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks". In: *Computers in Human Behavior* 139 (2023), p. 107551. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2022.107551. URL: https://www.sciencedirect.com/science/article/pii/S0747563222003715.

[66] Yuxiang Hong and Steven Furnell. "Understanding cybersecurity behavioral habits: Insights from situational support". In: *Journal of Information Security and Applications* 57 (2021), p. 102710. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2020.102710. URL: https://www.sciencedirect.com/science/article/pii/S2214212620308553.

[67] *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity: European Union Agency For Network and Information Security Report 2019*. Accessed 20-04.2024. 2019. DOI: https://doi.org/10.2824/324042. URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

[68] Dawn Branley-Bell et al. "Exploring Age and Gender Differences in ICT Cybersecurity Behaviour". In: *Human Behavior and Emerging Technologies* 2022 (Oct. 2022), pp. 1–10. DOI: 10.1155/2022/2693080.

[69] Duy Dang-Pham and Siddhi Pittayachawan. "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach". In: *Computers & Security* 48 (2015), pp. 281–297. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2014.11.002. URL: https://www.sciencedirect.com/science/article/pii/S0167404814001643.

[70] S Shyam Sundar and Sampada S Marathe. "Personalization versus customization: The importance of agency, privacy, and power usage". In: *Human communication research* 36.3 (2010), pp. 298–322.

[71] Tamir Mendel et al. “Toward Proactive Support for Older Adults: Predicting the Right Moment for Providing Mobile Safety Help”. In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6.1 (Mar. 2022). DOI: 10.1145/3517249. URL: https://doi.org/10.1145/3517249.

[72] Maryellen McClain Verdoes and Mahdi Nasrullah Al-Ameen. “Intermediate Help with Using Digital Devices and Online Accounts: Understanding the Needs, Expectations, and Vulnerabilities of Young Adults”. In: *HCI for Cybersecurity, Privacy and Trust: 4th International Conference, HCI-CPT 2022, Held as Part of the 24th HCI International Conference, HCII 2022, Virtual Event, June 26–July 1, 2022, Proceedings*. Vol. 13333. Springer Nature. 2022, p. 3.

[73] A. Bryman. *Social Research Methods*. OUP Oxford, 2012. ISBN: 9780199588053. URL: https://books.google.ee/books?id=vCq5m2hPkOMC.

[74] Damjan Fujs, Anže Mihelič, and Simon L. R. Vrhovec. “The Power of Interpretation: Qualitative Methods in Cybersecurity Research”. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. ARES ’19. Canterbury, CA, United Kingdom: Association for Computing Machinery, 2019. ISBN: 9781450371643. DOI: 10.1145/3339252.3341479. URL: https://doi.org/10.1145/3339252.3341479.

[75] Alicia O’Cathain, Elizabeth Murphy, and Jon Nicholl. “Three techniques for integrating data in mixed methods studies”. In: *BMJ* 341 (2010). ISSN: 0959-8138. DOI: 10.1136/bmj.c4587. eprint: https://www.bmj.com/content. URL: https://www.bmj.com/content/341/bmj.c4587.

[76] Benjamin James Knox. “Cyberpower Praxis: A Study of Ways to Improve Understanding and Governance in the Cyber Domain”. In: (2020).

[77] *Personal Data Protection Act*. Accessed 03.05.2024. URL: https://www.riigiteataja.ee/en/eli/523012019001/consolide.

[78] *Kaldi Offline Transcriber*. Accessed 25.01.2024. URL: https://github.com/alumae/kaldi-offline-transcriber.

[79] A. Joinson. Personal communication with the author. 04.01.2024.

[80] *About EUSurvey. EUSurvey*. Accessed 15.01.2024. URL: https://ec.europa.eu/eusurvey/home/about.

[81] *Help Page For Authors. EUSurvey*. Accessed 15.01.2024. URL: https://ec.europa.eu/eusurvey/home/helpauthors.

[82] *RV021: POPULATION BY SEX AND AGE GROUP, 1 JANUARY. Statistics Estonia*. Accessed 11.03.2024. URL: https://andmed.stat.ee/et/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV021.

[83] *Population Pyramid of Estonia: 2023. Statistics Estonia*. Accessed 11.03.2024. URL: https://www.stat.ee/rahvastikupyramiid/?lang=en.

[84] J. Pallant. *SPSS Survival Manual: A step by step guide to data analysis using SPSS*. Allen & Unwin Australia, 2011. ISBN: 9781742373928.

[85] Mohd Anwar et al. "Gender difference and employees' cybersecurity behaviors". In: *Computers in Human Behavior* 69 (2017), pp. 437–443. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2016.12.040. URL: https://www.sciencedirect.com/science/article/pii/S0747563216308688.

[86] Claire Seungeun Lee and Ji Hye Kim. "Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts". In: *Computers & Security* 97 (2020), p. 101995.

[87] Linda Little, Pamela Briggs, and Lynne Coventry. "Who knows about me? An analysis of age-related disclosure preferences." In: (2011).

[88] Matias Dodel and Gustavo Mesch. "An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices". In: *Computers & Security* 86 (2019), pp. 75–91. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.05.023. URL: https://www.sciencedirect.com/science/article/pii/S0167404818303080.

[89] Stefan Sütterlin et al. "The Role of IT Background for Metacognitive Accuracy, Confidence and Overestimation of Deep Fake Recognition Skills". In: *Augmented Cognition*. Ed. by Dylan D. Schmorrow and Cali M. Fidopiastis. Cham: Springer International Publishing, 2022, pp. 103–119. ISBN: 978-3-031-05457-0.

[90] *Digitaler Verbraucherschutz. Bundesamt für Sicherheit in der Informationstechnik (BSI).* Accessed 29.04.2024. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html.

[91] *Verbraucherinnen und Verbraucher: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen. Bundesamt für Sicherheit in der Informationstechnik (BSI).* Accessed 29.04.2024. URL: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen%5C-und%5C-Buerger%5C/buergerinnen%5C-und%5C-buerger%5C_node%5C.html.

[92] *Tu Ayuda en Ciberseguridad. Instituto Nacional de Ciberseguridad*. Accessed 29.04.2024. URL: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad.

[93] thinkSPAIN Team. *National online security helpline launched: 017*. Accessed 29.04.2024. 2019. URL: https://www.thinkspain.com/news-spain/31840/national-online-security-helpline-launched-017.

[94] Statistics Estonia. *Population census. 76% of Estonia's population speak a foreign language*. Accessed 29.04.2024. URL: https://www.stat.ee/en/news/population-census-76-estonias-population-speak-foreign-language.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Kati Sein

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Cybersecurity-related Support Needs and Challenges Incurred by Informal Support: a Study Among Estonian Home Users", supervised by Stefan Sütterlin and Tanel Mällo
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

11.05.2024

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview Guide in English

Interviewee no: .....

Start time: .....

Introduction

Hi, and thank you for participating in the study!

I am conducting this research as part of my Master's Thesis in cybersecurity programme at Tallinn Technical University. What interests me is a phenomenon in Estonia that, in home situations, laypeople turn to each other for getting cybersecurity and digital privacy-related advice and assistance.

I have prepared a set of questions and would like to record your answers. I am interested in both: your experiences (facts) as well as general opinions, views, assessemnts about the situation in Estonia. The data I gather upon your consent. It will be used only for this research and only by me; nothing identifiable about you or the people you mention will be published. Should I cite an utterance, interviewees will be referenced as Interviewee 1, Interviewee 2, etc. According to the Personal Data Protection Act, you have the right to withdraw your consent to participate in the study at any time, including during the interview.

About concepts and terms I will be using. I refer to people who perform cybersecurity support for their close ones as 'caregivers' ('nõustaja', 'abi andja', 'tugi'), and to receivers of such assistance as 'caregivees' ('hoolealune', 'abi saaja'). Terms 'home users', and 'laymen' ('tavakasutaja') refer to people using information technology in the home context where official IT/security assistance is not established. Opposite of this term is the organizational context where dedicated personnel for cybersecurity issues is established.

Before we start, do you have any questions for me?

Is it ok that I start the recording now? [*START RECORDING*]

Interview

1. First, I would note down some data about you.
   (a) Age: 16–24; 25–34; 35–44; 45–54; 55–64; 65–74; 75+
   (b) Gender: male, female, other, prefer not to say.
   (c) What is the highest level of school you have completed? no schooling completed, primary school, high/grammar school, trade/technical/vocational education, undergraduate, graduate, postgraduate
   (d) What is your field of study?
   (e) Describe your experience in cybersecurity or IT security?
2. Have you assisted anybody in a cybersecurity or privacy-related incident during 2022 or 2023? If yes, let's look at them more closely one by one. Please pick one and describe
   (a) What is your relation to the person who asked – a relative or friend or ...?
   (b) Age, gender, socio-economic situation of the person.
   (c) What did they ask – can you please describe their problem?
   (d) What was under threat in this situation?
   (e) What did you do to help them?
   (f) (*If it was a cyber incident*) Were you able to handle the incident "till the end" so that the problem was solved?
   (g) What do you think, in this particular situation, why did they ask you for assistance?
      i. If they did not have (access to) you – what would they have done then?

   (*Iterate this block of questions until no new instances come to mind.*)
3. Until now, we have talked about handling incidents, but there are also preventive measures to achieve and sustain a desired level of cybersecurity and/or privacy. Please recall situations when somebody approached you with questions that fall into this category.
   (a) What was asked?
   (b) Who asked? [Age, gender, socio-economic situation as before.]
   (c) Why did they ask you instead of using a source of official information?
4. What about Estonian e-services – have you been asked security-related questions about these? Has anyone needed assistance with these?
   (a) Has anyone asked for your assistance in casting their vote online at the parliament elections of 2023?
   (b) What about individual verification of one's i-vote – have you assisted anyone with this task? Was vote verification initiated by you or by them?
5. How often does it happen that people approach you with cyber-related questions or ask for help – once a week / a month / a year?

   (a) What is your experience – are cybersecurity and privacy issues asked explicitly, or do these topics arise among more general, IT-related situations?
   (b) Why do you help? What motivates you?
   (c) What principles do you have while performing assistance?
6. Do you feel confident while helping others?
   (a) Where do you get information to answer their questions?
   (b) Where do you get assistance when you have cyber-related problems yourself?
7. Do you proactively initiate discussions on cybersecurity or privacy within your community?
   (a) How do you do it?
   (b) What are the topics?
8. In your opinion, what are the characteristics of cybersecurity caregivees in Estonia: who ask for assistance from informal social networks instead of seeking official recommendations/assistance?
   (a) How would you describe cybersecurity concerns of laymen in Estonia?
   (b) What are the situations that Estonian home users fail to recognise as suspicious or dangerous?
   (c) Thinking of the awareness of laymen – is it the preventive domain or the reactive one where shortcomings are most critical?
   (d) In your opinion, what is the biggest problem or challenge in Estonian society in regard to cybersecurity?
9. Is low cyber hygiene of citizens bad? What is bad about it, what is at stake?

Closing

My prepared questions are over; thank you for answering them. If you know other people who provide informal assistance in IT and cyber-related issues as you do, I would be glad if you shared my contacts with them so they can decide whether to participate in the study.

Perhaps I missed an important aspect that you'd like to share? Is there anything you want to add? [*Iterate.*]

Thank you! I will now stop recording. [*STOP RECORDING*]

End time of interview: .....

Appendix 3 – Detailed Findings of the Qualitative Study

Reactive support – Topics. The interviews always started with asking the interviewee to describe cases when a caregivee took an active stance and asked them for help in a cybersecurity incident or placed them a question.

As of incidents, giving advice to victims of phishing emails and helping them regain access to or close compromised accounts were both reported by three interviewees. Recovering Facebook accounts was standing out in this regard (Interviewee 3: "There have been very many cases."), Steam and email accounts were also mentioned. Five interviewees said they had been asked to diagnose whether a mail is legitimate or should be treated as spam or phishing. Interviewee 3 noticed that these requests usually come from young people in their twenties or even younger, with the youngest being 13 years old. They explain that young people do not yet have enough experience with emails. Interviewee 5 points out that, in 2023, scam emails have become more credible. Questions about good passwords and password management came up in 4 interviews: what is the length of a good password? Which password manager should one choose? How to use a password manager? Interviewee 7 described that their caregivee regularly calls them to help recall passwords and PIN codes (e.g., email, phone, smartwatch). Besides forgetting one's credentials, the challenge is distinguishing whether the device, SIM card or account PIN should be typed in. Two interviewees described that devices are often brought for inspection ("My computer has become slow, please fix it."). One interviewee has been often asked about the privacy and security settings of Facebook and Twitter. They also described a caregivee in their forties asking them to choose their new phone's privacy and security settings. Another interviewee was asked whether the original photo would be uploaded to social media when the intent was to upload a redacted version. People also ask whether a service, platform, app, or device "is secure," e.g. TikTok. One interviewee expressed concern that people, instead of asking about the security of devices, ask which one is better and then buy the cheapest despite any recommendations.

Reactive support – Timing. Interviewees pointed out that cybersecurity questions arise in the general information technology context. "Nobody approaches me with specific cybersecurity issues. Computers break down in normal use, something goes wrong, something has to be changed"(Int6), or "people are more likely to have problems not with

security, but with data loss or other technological problems: something is not working, they say, “My phone is dead” or “My computer is dead.” Cybersecurity questions are asked very seldom (Int2).

Proactive support – Topics. Next, the interviews focussed on cases when the interviewees had been in a proactive role, e.g., initiating conversations or cybersecurity caregiving sessions. Three interviewees described showing phishing emails to their caregivees, pointing to indicative characteristics of these and demonstrating detection techniques (e.g., hovering over link). Three interviewees promoted the implementation of multi-factor authentication. Two interviewees said they taught long passwords and the usage of a password manager. Proper use of password manager was so crucial in the eyes of one of them that if they could choose only one recommendation, then this would be the one they advocated for. However, they sadly admitted people would not adopt it since it requires a change in user behaviour and takes a month to set up and change old, weak passwords, account by account. Two interviewees said they promote using an ad blocker to prevent falling victim to scam campaigns. Interviewee 6 added, “I’m not happy that I have to block what is essentially the only source of income for websites, but I find I have no choice.” Two interviewees said they, for privacy concerns, advocate the Linux operating system among their caregivees, and one of them recommends the e Foundation operating system for smartphones.[1]

Concern about using privacy-invasive apps was expressed by two interviewees, so they recommend avoiding such apps and paying attention to permissions apps require. One of them additionally expressed disapproval of parents sharing photos of their children or making social media accounts for minors. They investigate and then explain the privacy policies of apps that modify photos uploaded by users (e.g., turning the portrayed person significantly older or presenting them as Barbie or Ken) to their social circles. One interviewee said that whenever they notice someone not deploying a screen lock on their phone, they intervene politely by asking for reasons not using it and explaining why a screen lock is helpful from their point of view. One interviewee recommended that one avoid unknown cloud services. Explaining cryptography and the underlying principles for Estonian e-government services was often carried out by one interviewee.

Proactive Support – Timing. Two interviewees said that they explain and initiate the application of security controls in the recovering phase of an incident. For example, when a hijacked account is successfully restored, they apply two-factor authentication with the cybersecurity caregivee. Shortly after falling victim to a phishing email, the time was

[1] eOS is a complete, fully “deGoogled”, mobile ecosystem. Accessible at https://e.foundation/e-os/. Accessed 25.04.2024.

utilised to re-address what characteristics of an email should make one cautious. One caregiver shared that when paying a visit to the caregivee (a relative), they always inspect the status of updates and anti-virus software on their computer. Another said they had adjusted the settings of their parent's home router and ensured all computers had security updates installed and set as automatic. They pointed out that they perform this task only with their parents; proposing it to their friends would feel too invasive.

Sharing links to articles and news items on cybersecurity was a common practice of three interviewees. One of them posts news and shares information on her social media wall. Another shared how they often raise cybersecurity-related discussions at a dinner table, pointing out that Christmas time and other festivities when relatives and friends come together are fruitful periods in the year; besides, new devices are received as gifts. Drawing examples from their own life (e.g., a recently received phishing email) or reflecting on a recent blog post helps to create context. Once the context is established, people get interested and ask various questions. This way, they have raised people's interest and discussions on, for example, how the Estonian ID-card and DigiDoc software work, how files are encrypted and decrypted, the privacy settings of Nintendo Switch, and good passwords and their management. "I have not encountered a person who cannot come up with a question about passwords when they learn that I work as a security engineer.

Proactive support – Strategies, activities As for other successful strategies on how to get people to think along with security issues, one interviewee shared an observation that people like problems but not solutions. Asking intriguing questions like "How much would you pay to get back the photos of your relatives?" or "Would you pay ransom to the attackers?" or "Would you trade your encrypted photos for forwarding the virus to two more people?" make people consider possible solutions which are interesting for them. Cybersecurity deals mainly with providing solutions and not catching people's attention with such problems and dilemmas.

To make people consider adopting a password manager, one interviewee asked how many accounts they had. The quick answer he gets is five, and then they start recalling and realising they have too many accounts even to remember their existence. Additionally, they shared that what had worked well for them was understanding that practising good cyber hygiene "has been cyber culture: it is cool when you use more secure services, act more cautiously." They elaborate further that the possibility of using a password manager in the Estonian language might encourage some people to adopt it.

Performing party tricks to get people to think along with cybersecurity topics belongs to the manners of another interviewee claiming that "what actually affects people is

demonstration." A personal, painful experience is most effective, but stories of other people's experiences should have a good impact.

Cybersecurity caregivers try to nudge their cybersecurity caregivees to learn to make decisions and configure the devices independently. "I am trying to teach people to be more and more self-reliant. For example, if I find an answer immediately on the Internet, I encourage people to look for it themselves and hope they find the same answer. If I know the answer, I motivate them to find it. But first, I have to know the answer myself beforehand." (Int2). Another interviewee said they avoid touching the cybersecurity caregivee's device at all – for the person to make their own choices and learn. "Whenever possible, I try to ensure I don't touch the person's device. First, if a person goes through the steps, he remembers better. Secondly, if he does it himself, he understands what he is doing; if he doesn't understand, he doesn't do it. [—] Then he makes the choice himself. I can give a suggestion, but I can't force him to do anything." (Int3)

Reactive And Proactive Support – Principles. The interviewees told how they first try to figure out the security needs (or model) of the cybersecurity caregivee. For example, in response to whether this or that thing is secure, the caregiver tries to understand what they fear would harm them the most. Some interviewees said they try to guess and predict it. One said they would find it out by asking questions. Interviewees claimed they would not impose their own preferences but would try to base their recommendations and assessments on the situation of the person asking. "For me, security issues always start with analysing what is to be secured in the first place, for what purposes and against whom. [—] However, in recommending a password manager, I asked if the goal would be that no one can access your encrypted passwords or whether you accept the risk that someone will see the encrypted data. The caregivee accepted that risk because the availability of those is better, so he decided on the cloud solution (Int3)". A principle that security measures are explained from the point of view of the cybersecurity caregiver themselves, not from the cybersecurity caregivee was another principle: "because I may not know their challenges in life"(Int3). There are things that caregivers state they would never do. Although asked, they would never unlock a device by bypassing the locking mechanism set on the device (Int3) or bypassing the paywall of a news portal (Int5).

Concerns – Attitudes. One source of the weak security posture of laypeople is seen in the fact that they value convenience and a plethora of features over security (Int2). Also prevailing is the people's attitude that there is nothing to take from them, and if there is something to take, other methods protect this, e.g. the bank has its methods to make sure the right person gets money from the correct account (Int3).

Interviewee 2 dreams of a population that would try to be more autonomous in how they handle their data, claiming they tend to use cloud services without thinking about privacy. “Independence is an important prerequisite when we want to talk about security. [—] It takes an awful lot of effort to achieve any independence in IT tools. Having that Independence regarding your data or how you use the Internet is very hard. But then to do it all securely!” (Int2)

Shortcomings are seen in the attitudes of the training security experts, too. Offering offensive security courses instead of teaching how to defend effectively they encourage the mindset that cybersecurity and defending are boring, whereas hacking is cool. “Among the courses and certificates available on the market in Estonia, five address offensive security, teaching you how to attack and half of a course teaches you how to defend. The ratio is a bit out of place. For example, how to set up a web server so that it doesn’t fall down under a DDoS attack? One simple module that protects you against most injection attacks – this could be an elementary skill. How to securely set up and manage an email server? If you write Python code and include a library - how many repositories do you actually include? (Int2).

Concerns – Practices and lack of practices. As of practices that need to be changed, the habit of introducing smartphones with default settings (Int3), impulsive clicking (Int2, Int5) and lack of critical thinking (Int5) were brought forth. Interviewee 5 noted that being an extensive computer user does not protect against bad practices. Interviewee 6 mentioned that, although simple means to make passwords stronger, the existence of passphrases is not acknowledged. According to them, the adoption of password managers would make the biggest enhancement in the cybersecurity posture of the population. Cybersecurity caregivers recognise that awareness is not bad among Estonians at all; the question is how to really make people practice cyber hygiene (Int6). "Whatever is said, whatever controls are recommended no one will listen until the bang goes off. Then maybe some extra protection is put on the new account," concludes Interviewee 5.

Concerns – Inevitables. Interviewee 3 observes that there are not many places where ordinary people can get information on security so that an average person would know what to do before introducing a new phone. They claim that laypeople necessarily do not feel secure; rather they understand that cybersecurity is an issue, they have an interest and would take time to read articles and opinions. However, they give recognition to the Be IT-conscious! awareness campaign. A certain amount of experience is needed to recognise a suspicious site, email or behaviour, one should be familiar with what normality looks like, said Interviewee 4. This was confirmed by Interviewee 3, who observed that minors and young people often lack experience with how a typical email should look. The learning

curve for starting to use a password manager is steep, and this keeps people from adopting it, as mentioned in Interviewee 6.

Concerns – Consequences to state and society. Cybersecurity caregivers described negative outcomes of the population's weak cyber hygiene. When people lose money on a massive scale, it is also a direct cost to the state, inferred Interviewee 6. Interviewee 7 explained that while gaining access by breaking cryptography is difficult, it is much easier to gain access by influencing the user (including employees) through social attacks. "By practising digital hygiene, one makes themselves not so easily attacked. The weaker the digital hygiene, the easier it is to gain access. Damage can be done to the individual, the company, and the state, depending on whose systems were accessed by that user." (Int7)

Also, reputational damage to the state was envisaged in interviews. As Interviewee 6 put it, "For us specifically, it is absolutely about reputation, too. One of the things we talk proudly about in the world is our e-government. If we have great e-government, we could have people who are more educated on average – which I don't know, maybe we are?" Interviewee 7 warned that it is easy to damage and difficult to restore the country's reputation by recalling the ID card crisis, which was resolved quickly and relatively successfully, but the reputational stigma still prevails. Interviewee 4 emphasised that if the state has built up all its activities and functions if it has built up all its services in the cyber world, that is, on the Internet, then inevitably, it has to guarantee its citizens that all these services will function in such a way that no harm will result for them from their use.

Appendix 4 – Survey Questionnaire in Estonian

Hea vastaja!

Olen Tallinna Tehnikaülikooli küberkaitse magistriprogrammi üliõpilane. Minu uurimistöö teema on Eesti inimeste toimetulek küberturvalisusega eraelus – hakkama saamine isiklike seadmete ja kontode turvalisena hoidmisega olukordades, kus abi andmine ei ole kellegi töökohustus. Käesoleva küsimustikuga uurin, milliste küberhügieeni toimingute juures ja milliste küberohtudega kokkupuutel eelistatakse küsida abi teiselt inimeselt, kas inimestel on, kellelt abi küsida, ja mis iseloomustab sellist abi andja ning küsija vahelist suhet.

Uurimistöö tarbeks kogun ainult isikustamata andmeid. Palun ärge avaldage isikut tuvastada võimaldavat teavet enda ega kellegi teise kohta. Andmeid kasutan magistritöö ja võimaliku teaduspublikatsiooni kirjutamisel. Käesoleva uurimuse tulemusi saate vaadata Tallinna Tehnikaülikooli digikogus (digikogu.taltech.ee) avaldatavast magistritööst hiljemalt 2024. aasta sügisel.

Vastama on oodatud täisealised Eesti kodanikud ja residendid. Vastamisele kulub umbes 15 minutit. Küsimustik on avatud 31. jaanuarini 2024 kl 23:45.

On suurepärane, kui jagad küsimustikku ka oma tuttavatele ja sugulastele. Mida rohkem vastajaid, seda täielikuma pildi Eesti inimeste toimetulekust oma seadmete ja kontode küberturvalisusega ma oma töös saan.

Q1. Teie vanus – 18-24, 25-34, 35-44, 45-54, 55-64, 65-74, 75 või vanem
Q2. Teie sugu – mees, naine, muu, eelistan mitte öelda
Q3. Haridus – põhiharidus, gümnaasiumiharidus või keskharidus, kutseharidus, kõrgharidus, eelistan mitte öelda
Q4. Kas Te olete praegu peamiselt – töötav, töötu, pensionär (vanadus-, ennetähtaegsel või sooduspensionil), osalise või puuduva töövõimega mittetöötav (endine töövõimetuspensionär), õpilane või üliõpilane, kodune, ajateenija või asendusteenistuja, muu
Q5. Mitu tundi nädalas keskmiselt kasutate internetti **töö- või kooliülesannete täitmiseks** (arvuti, telefoni või muu seadme abil)? – kuni 10 tundi, 11 kuni 20 tundi, 21 kuni 40 tundi, 41 ja rohkem tundi
Q6. Mitu tundi nädalas keskmiselt kasutate internetti **muuks otstarbeks** kui tööülesannete täitmiseks (näiteks sotsiaalmeedia, uudised, meelelahutus, kaubandus jne)? –

kuni 10 tundi, 11 kuni 20 tundi, 21 kuni 40 tundi, 41 ja rohkem tundi

Järgnevatele kolmele küsimusele (Q7, Q8, Q9) vastates mõelge olukordadele, mis võivad ette tulla eraelus isiklike seadmete ja kontode kasutamisel, kus abi andmine ei ole kellegi töökohustus. – Küsiksin kohe; Küsiksin, kui kiire otsing internetist ei vii lahenduseni; Küsiksin, kui põhjalik otsing internetist ei vii lahenduseni; Ei küsiks, isegi kui ise lahendust ei leia; Ei küsiks, sest oskan seda teha; Ei saa küsimusest aru

Q7. Küberohud ja -intsidendid. **Millistes neist olukordadest Te küsiksite abi või nõuannet teiselt inimeselt?**
   (a) Mul ei õnnestu sisse logida oma sotsiaalmeedia kontole ja kahtlustan, et see on üle võetud.
   (b) Mul ei õnnestu sisse logida oma e-posti kontole ja kahtlustan, et see on üle võetud.
   (c) Sisestasin oma PIN-koodid veebilehele, mis võis olla õngitsusleht.
   (d) Smart-ID või Mobiil-ID abil sisse logides kuvab telefon teist kontrollkoodi kui veebileht, millelt sisselogimise algatasin.
   (e) Soovin teavitada küberohust või -kuriteost (nt õngitsuskampaania, küberkius, identiteedivargus).
   (f) Mu failid ei avane ja näen kirja, et need on krüpteeritud ja nõutakse raha.

Q8. Küberturvalisust parandavad tegevused. **Millistes järgmistes olukordades Te küsiksite abi või nõuannet teiselt inimeselt?**
   (a) Soovin hakata kasutama paroolihaldurit.
   (b) Soovin oma kõige olulisematele kontodele seadistada mitmefaktorilise autentimise.
   (c) Soovin saaja nimele krüpteerida tundlikku infot sisaldav fail.
   (d) Soovin aru saada oma nutiseadme või konto turvaseadistusest.
   (e) Soovin välja selgitada, kas tegemist on ohutu lingiga.
   (f) Soovin välja selgitada, kas tegemist on ohutu e-kirja või sõnumiga.
   (g) Soovin välja selgitada, kas veebileht, millele oma andmeid sisestan, on selleks piisavalt turvaline.
   (h) Soovin muuta oma kodus oleva ruuteri nähtavust, nime või parooli.
   (i) Soovin hoida silma peal oma kodust ruuterit läbival liiklusel.
   (j) Soovin aru saada, kas mu seadmesse on sisse murtud.
   (k) Soovin aru saada, kas mõnda mu kodustest seadmetest (nt turvakaamera, beebimonitor vm) kasutatakse küberründes.

Q9. Andmete kogumine ja kasutamine. **Millistes neist olukordadest Te küsiksite kellegi abi või nõuannet?**
   (a) Tahan teada, kes on minu kohta andmeid küsinud Eesti e-riigi andmekogudest

(nt tervise infosüsteem, e-maksuamet).

(b) Tahan teada, milliste Eesti registrites ja infosüsteemides olevate andmete kasutamiseks olen andnud nõusoleku.

(c) Tahan teada, milliseid nõusolekuid olen oma andmete kasutamiseks andnud veebilehitsejates kolmandatele osapooltele.

(d) Tahan teada, milliseid andmeid mõni minu seade kogub ja edasi jagab.

(e) Tahan piirata oma seadmetes ja äppides mulle sobimatut andmete kogumist.

Q10. Kui neis loeteludes oli puudu mõni olukord, milles abi või nõu küsiksite, siis palun lisage.

Q11. Kui vajate eralus abi küberturvalisuse alases küsimuses, siis mis on Teie arvates sellise abi saamisel oluline? Valige 3 kuni 4 kõige olulisemat tegurit.

(a) Abi on võimalik saada kiiresti.

(b) Abi on asjakohane ja täpne.

(c) Abi andja toetub ametlikele allikatele.

(d) Abi küsija ei pea abi andjale oma olukorda selgitama, see on talle tuttav.

(e) Abi on võimalik saada abi andjaga samas ruumis.

(f) Abi küsija saab abi andja selgitustest aru.

(g) Abi andja on diskreetne.

(h) Abi küsija ei pea ise lahenduse jaoks süvenema.

(i) Abi on tasuta.

(j) Abi küsimine on lihtne.

(k) Abi kättesaadav kellaajast sõltumata.

Q12. Kui mõni oluline tegur on puudu, siis võite lisada.

Q13. Kas Teie perekonnas või tutvusringkonnas on inimesi, kelle poole pöördute või saaksite pöörduda, kui Teil on eraelus küberturvalisuse alane küsimus või lahendamist vajav olukord? –

(a) Jah, on inimesi, kelle poole saan pöörduda. – Jätkake küsimusega Q15.

(b) Ei, ei ole selliseid inimesi.

Q14. Kas tunnete sellise inimese järele vajadust, kelle käest eraelus ette tulevates küberturvalisuse alastes küsimustes nõu või abi küsida?

(a) Jah. – Jätkake küsimusega Q22.

(b) Ei. – Jätkake küsimusega Q22.

Q15. Mida Te väärtustate tuttava või sugulase käest saadud abi juures? Valige 3 kuni 4 kõige olulisemat tegurit.

(a) Ta annab abi kiiresti.

(b) Tema antud abi on asjakohane ja täpne.

(c) Abi andes toetub ta ametlikele allikatele.

(d) Ma ei pea talle oma olukorda selgitama, see on talle tuttav.

(e) Saan abi, olles temaga samas ruumis.

(f) Saan tema selgitustest aru.
(g) Ta on diskreetne.
(h) Ma ei pea ise lahenduse jaoks süvenema.
(i) Tema nõu ja abi on tasuta.
(j) Temalt on lihtne küsida.
(k) Saan tema abi küsida kellaajast sõltumata.

Q16. Kui mõni oluline tegur on puudu, siis võite lisada.

Q17. Kas praegu saate **eraelus** tekkinud küberturvalisuse alastes küsimustes abi piisavalt?
(a) Jah.
(b) Ei.
(c) Võib-olla.

Q18. Kas olete mingil põhjusel jätnud tuttava või sugulase käest abi küsimata?
(a) Jah, olen.
(b) Ei, ei ole. – Jätkakte küsimusest Q21.

Q19. Mis põhjusel jätsite küsimata?
(a) Mul oli piinlik.
(b) Arvasin, et teen talle tüli.
(c) Otsustasin ise lahenduse/vastuse leida.
(d) Loobusin olukorra lahendamisest või küsimusele vastuse otsimisest.

Q20. Kui mõni oluline põhjus jätta abi küsimata on eelnevast loetelust puudu, siis võite lisada.

Q21. Kui keegi Teid eraelus küberturvalisuse küsimuses aitab, kes sisestab info seadmesse?
(a) Mina.
(b) Abi andja.
(c) Abi andja, aga ma näen ja saan aru, mida ta teeb.
(d) Mõlemad, sealjuures ma näen ja saan aru, mida ta teeb.
(e) Mõlemad, sealjuures ma ei näe või ei saa aru, mida ta teeb.
(f) Ei saa küsimusest aru.

Q22. Olukord, kus küberturvalisuse osas aidatakse teineteist tutvuse poolest (sugulane, sõber, tuttav), võib sisaldada ohte. **Milline järgnevatest olukordadest on Teie elus juba juhtunud?** – Jah, on juhtunud; Ei, ei ole juhtunud; Ei ole kindel
(a) Abi andja andis halba nõu.
(b) Abi saajana muutusin abi andjast sõltuvaks.
(c) Abi andja sai minu kohta teada tundlikku infot.
(d) Abi andja sai teada minu PIN-koodid või parooli.
(e) Abi andja sisenes minu kontole (nt pangakonto, e-postkast).
(f) Abi andja tegi minu teadmata minu nimel toiminguid.

Q23. **Kui võimalikuks peate järgnevate olukordade tekkimist Teie elus tulevikus?** – Täiesti võimatu; Pigem võimatu; Ei oska vastata; Pigem võimalik; Täiesti võimalik

(a) Abi andja annab halba nõu.
(b) Abi saajana muutun abi andjast sõltuvaks.
(c) Abi andja saab minu kohta teada tundlikku infot.
(d) Abi andja saab teada minu PIN-koodid või parooli.
(e) Abi andja siseneb minu kontole (nt pangakonto, e-postkast).
(f) Abi andja teeb minu teadmata minu nimel toiminguid.

Q24. Kui eelnevas loetelus puudub mõni oluline oht, mis võib peituda olukordades, kus küberturvalisuse küsimustes aidatakse teineteist tutvuse poolest, siis palun lisage.

Q25. Üks olukord, kus küberturvalisus on kriitilise tähtsusega, on e-hääletamine. Kas Te olete e-hääletanud?
(a) Jah, olen e-hääletanud.
(b) Ei, ei ole e-hääletanud. – Jätkake küsimusega Q27.

Q26. Järgnevalt on toodud olukorrad, mis võivad tekkida e-hääletamise juures. **Kas Teie elus on juhtunud mõni neist olukordadest?** – On juhtunud; Ei ole juhtunud; Ei saa küsimusest aru
(a) Keegi on mind e-hääletamise juures abistanud.
(b) Keegi on vastu minu tahtmist üritanud teada saada, kelle poolt ma e-hääletasin.
(c) Keegi on mulle e-hääletamise juures oma eelistust peale surunud.

Q27. Igapäevases elus võime kokku puutuda erinevate küberohtudega. **Palun hinnake, mil määral iseloomustavad allpool toodud laused Teie tundeid ja mõtteid küberohtu sisaldavates olukordades?** (Mõned väited võivad tunduda korduvat, aga see on vajalik.) – Ei ole üldse nõus; Pigem ei nõustu; Ei oska öelda[1]; Pigem nõustun; Olen täiesti nõus
(a) Suudan oma seadmeid hoida turvalisena.
(b) Usun, et ma saan küberohte sisaldavate olukordadega hakkama.
(c) Tulen küberohtu sisaldavates olukordades hästi toime.
(d) Tean, et suudan lahendada enamiku küberturvalisusega seotud probleemidest.
(e) Ebaõnnestumine mõjub mulle heidutavalt.
(f) Sellises olukorras ei näe ma mõtet proovidagi.
(g) Tunnen end sellises olukorras abitult.
(h) Sellised probleemid tunduvad võimatud lahendada.
(i) Mul on sõpru või perekonnaliikmeid, kes saavad mind ohtudega toime tulemisel aidata.
(j) Mu tutvusringkonnas on inimesi, kes oskavad mind probleemiga tegelemise juures toetada.
(k) Mul ei ole ühtki tehnilise taibuga sõpra, kes saaks abiks olla.
(l) Mul pole kedagi, kelle poole abi saamiseks pöörduda.

[1] In the survey, the wording "Ei soovi öelda" ("Do not wish to say") was used by mistake. The correct neutral option would be "Cannot say" as provided above.

(m) Minu jaoks on küberohtu sisaldavad olukorrad kogemused, millest õppida.
(n) Kogemused küberohtudega aitavad mul õppida pingelises olukorras toime tulema.
(o) Käsitlen küberohte sisaldavaid olukordi väljakutsetena.
(p) Saan kogemusi küberohtudega kasutada enesearenguks.

Q28. Järgnevad käitumisjuhised on saadud konsulteerides veebikonstaabli, Riigi Infosüsteemi Ameti, küberturvalisuse ekspertide ning Smart-ID ja Mobiil-ID kasutajatugedega. **Milliseid järgnevatest soovitustest teadsite juba enne siit lugemist?** – Teadsin; Teadsin ja olen kasutanud; Kuulen sellest esimest korda
(a) Kui Teile tuleb tuttavalt kiri, mida Te ei oodanud ning milles ta palub avada manus või vajutada lingile, siis selle kirja ohutuses veendumiseks küsige sellelt inimeselt mõne muu kanali kaudu üle, kas ta tõesti saatis selle kirja.
(b) Kui manust või linki sisaldava kirja saadab Teile võõras, siis kontrollige nende ohutus selleks loodud virtuaalses keskkonnas, nt VirusTotal www.virustotal.com.
(c) Kui soovite veenduda, kas kuvatav link ja avatav link on samad, minge hiirega lingile ning kopeerige link parema klõpsuga, kleepige see tekstiredaktorisse ja võrrelge kirjas kuvatavaga.
(d) Kui Smart-ID või Mobiil-ID abil sisse logides kuvab telefon muud kontrollkoodi kui veebileht, millelt sisselogimise alustasite, katkestage sisselogimine, taaskäivitage telefon ja proovige uuesti. Kui ka teisel katsel kontrollkoodid ei kattu, siis informeerige olukorrast vastavalt Smart-ID või mobiil-ID teenuse pakkujat ja oodake juhiseid.
(e) Kui kahtlustate, et keegi teine esineb veebis Teie nime all või olete sattunud kiusamise või ahistamise ohvriks, on kõige õigem teavitada oma piirkonna veebipolitseinikku, kelle kontaktid leiab www.politsei.ee/et/piirkonnapolitsei.
(f) Kui puutute kokku küberkuriteoga (konto ülevõtmine, lunavararünnak, raha vargus pangakontolt vms), siis teatage sellest politseile aadressil cyber.politsei.ee.

Q29. Kas oskate kontrollida, kas ülalpool toodud kolm linki on ohutud ja viivad just neile lehtedele, kuhu näiliselt lubavad?
(a) Jah.
(b) Ei.

Q30. Kas selle küsimustiku vastamisel aitas Teid keegi?
(a) Jah.
(b) Ei.

Q31. Sellega on kõik küsimused vastatud. Kui soovite midagi lisada või tagasisidet anda, siis seda saadte teha selles tekstiväljas.

Appendix 5 – Survey Questionnaire in English

Dear Respondent,[1]

I am a student in the Cybersecurity Master's programme at Tallinn University of Technology. My research topic is how people in Estonia cope with cybersecurity in their personal lives - how to keep personal devices and accounts secure in situations where it is not someone's job to help. With this questionnaire, I am investigating which cyber hygiene activities and cyber threats people prefer to ask another person for help with, whether people have someone to ask for help from, and what characterises this kind of help-giver/helper relationship.

For this research, I will collect only impersonal data. Please do not disclose the identity of the personally identifiable information about yourself or anyone else. I will use the data for my thesis and a possible research publication. You can download the results of this research data from the master thesis to be published in the digital collection of Tallinn University of Technology (digikogu.taltech.ee) at the latest in autumn 2024.

Adult Estonian citizens and residents are invited to respond. It will take approximately 15 minutes. The questionnaire is open until 5 February 2024 at 12:00.

It would be great if you share the questionnaire with your friends and relatives. The more respondents, the more complete picture of how people in Estonia are managing the cybersecurity of their devices and accounts I achieve with my work.

Q1. Your age – 18-24, 25-34, 35-44, 45-54, 55-64, 65-74, 75 or older
Q2. Your gender – male, female, other, prefer not to disclose
Q3. Education – primary education, grammar school, vocational education, higher education, prefer not to say
Q4. Are you currently mainly – employed, unemployed, retired (old-age, early retirement or pension), partially or disability inactive (formerly disability pensioner), pupil or student, housewife/househusband, recruit, other
Q5. On average, how many hours a week do you use the internet for **tasks related to your work or schooling** (by computer, phone or other device)? – up to 10 hours, 11

[1]Translated from Estonian into English using DeepL Translator neural machine translation service (free version) accessible at https://www.deepl.com/translator. Accessed 30.01.2024.

to 20 hours, 21 to 40 hours, 41 and more hours

Q6. On average, how many hours a week do you use the internet for **tasks other than** work or schooling (e.g., social media, news, entertainment, e-commerce, etc.)? – up to 10 hours, 11 to 20 hours, 21 to 40 hours, 41 and more hours

When answering the following three questions (Q7, Q8, Q9), think about situations that might occur in your private life when using personal devices and accounts where it is not someone's job to help you. – Would ask immediately; Would ask if a quick search on the internet does not lead to a solution; Would ask if a thorough search on the internet does not lead to a solution; Would not ask even if I cannot find a solution; Would not ask because I know what to do / because I can do it; Do not understand the question.

Q7. Cyber threats and incidents. **In which situations would you ask another person for help or advice?**
   (a) I can't sign in to my social media account and suspect it has been taken over.
   (b) I can't log in to my email account and suspect it has been taken over.
   (c) I entered my PINs on what could have been a fishing website.
   (d) When signing in with Smart ID or Mobile ID, my phone displays a different verification code than the webpage from which I initiated the process.
   (e) I want to report a cyber threat or crime (e.g. phishing campaign, cyberbullying, identity theft).
   (f) My files won't open, and I see a message saying these are encrypted and money asked.

Q8. Actions to improve cybersecurity. **In which situations would you ask another person for help or advice?**
   (a) I need to start using a password manager.
   (b) I need to set up multi-factor authentication for my most important accounts.
   (c) I need to encrypt a file containing sensitive information in the name of the recipient.
   (d) I need to understand the security settings on my smart device or account.
   (e) I need to find out if this is a safe link.
   (f) I need to find out if this is a safe email or message.
   (g) I need to find out if the website I am entering my data on is secure enough to do this.
   (h) I need to change my home router's visibility, name or password.
   (i) I need to monitor traffic passing through my home router.
   (j) I need to find out if my device has been hacked.
   (k) I need to find out if any of my home devices (e.g. security camera, baby monitor, etc.) are being used in a cyber attack.

Q9. Data collection and use. **In which of these situations would you ask another person for help or advice?**
   (a) I want to know who has requested data about me from Estonian e-government databases (e.g. Health Information System, e-Tax Board).
   (b) I want to know which data in Estonian registers and information systems I have consented to use.
   (c) I want to know what consents I have given to third parties for using my data in web browsers.
   (d) I want to know what data some of my devices collect and share.
   (e) I want to limit inappropriate data collection on my devices and apps.

Q10. If there was a situation missing from these lists that you would like help or advice on, please add it.

Q11. If you need help with a cybersecurity issue in your private life, what aspects do you think are important in getting such help? Please select the 3 to 4 most important factors. (Random order)
   (a) Help is available quickly.
   (b) The help is relevant and accurate.
   (c) The helper relies on official sources.
   (d) The person asking for help does not need to explain their situation to the person providing the help, it is familiar to them.
   (e) It is possible to get help in the same room as the provider.
   (f) The person asking for help understands the explanations given by the person giving help.
   (g) The helper is discreet.
   (h) The person asking for help does not need to delve into the solution themselves.
   (i) The help is for free.
   (j) Asking for help is easy.
   (k) Help is available regardless of the time of day.

Q12. If any important factor is missing, you can add it.

Q13. Are there people in your family or acquaintances that you turn to or could turn to if you have a cybersecurity issue or situation in your personal life that needs to be resolved?
   (a) Yes, there are people I can turn to. – Continue with Q15.
   (b) No, there are no such people.

Q14. Do you feel the need for someone to turn to for advice or help with cybersecurity issues in your private life?
   (a) Yes. – Continue with Q22.
   (b) No. – Continue with Q22.

Q15. What do you value in the help you receive from a friend or relative? Please select

the 3 to 4 most important factors. (Random order)

(a) They provide help quickly.
(b) The help they give is relevant and accurate.
(c) They rely on official sources when helping.
(d) I don't need to explain my situation to them, they are familiar with it.
(e) I can get help in the same room with them.
(f) I understand their explanations.
(g) They are discreet.
(h) I don't need to delve into the solution myself.
(i) Their advice and help are for free.
(j) It is easy to ask them.
(k) I can ask for help regardless of the time of day.

Q16. If any important factor is missing, you can add it.

Q17. Are you currently getting enough help with cybersecurity issues in your **private life**?

(a) Yes.
(b) No.
(c) Maybe.

Q18. For whatever reason, have you held back from asking a friend or relative for help?

(a) Yes, I have.
(b) No, I have not. – Continue with Q21.

Q19. Why did you hold back from asking?

(a) I was embarrassed.
(b) I thought I disturbed them.
(c) I decided to find the solution/answer myself.
(d) I refrained from resolving the situation or seeking an answer.

Q20. If an important reason for not asking for help is missing from the above list, you can add it.

Q21. When someone is helping you privately with cybersecurity, who enters the information into the device?

(a) Me.
(b) The helper.
(c) The helper, but I see and understand what they are doing.
(d) Both, but I can see and understand what they are doing.
(e) Both, but I cannot see nor understand what they are doing.
(f) Do not understand the question.

Q22. A situation in which a private person assists another private person may contain threats. **Which of the following situations has happened in your life?** – Yes, it has happened; No, it has not happened; Not sure

(a) The helper gave bad advice.

(b) As a help receiver, I became dependent on the helper.
(c) The helper learned sensitive information about me.
(d) The helper learned my PIN code or password.
(e) The helper logged into my account (e.g., bank account, mailbox).
(f) Without my knowledge, the helper took action on my behalf.

Q23. **How likely do you think the following situations are to occur in your life in the future?** – Totally impossible; Somewhat impossible; Cannot say; Somewhat possible; Totally possible
(a) The helper will give bad advice.
(b) As a help receiver, I will become dependent on the helper.
(c) The helper will learn sensitive information about me.
(d) The helper will learn my PIN code or password.
(e) The helper will log into my account (e.g., bank account, mailbox).
(f) Without my knowledge, the helper will take action on my behalf.

Q24. If the above list misses a significant risk inherent in situations where a private person assists another in cybersecurity issues, please add it.

Q25. One situation where cybersecurity is critical is i-voting. Have you i-voted?
(a) Yes, I have i-voted.
(b) No, I have not i-voted. – Continue with Q27.

Q26. The following are situations that may arise at i-voting. **Have any of these situations happened in your life?** – Has happened; Has not happened; Do not understand the question
(a) Someone has helped me with i-voting.
(b) Someone has been trying, against my will, to find out who I i-voted for.
(c) Someone has coerced me at i-voting.

Q27. In our daily lives, we are exposed to various cyber threats. **Please rate the extent to which the sentences below describe your feelings and thoughts in cyber threat situations.** (Some of the arguments may seem repetitive, but it is necessary.) – Disagree; Somewhat disagree; Don't want to say; Somewhat agree; Strongly agree (Random order)
(a) I can keep my devices secure.
(b) I believe in myself to deal with it.
(c) I am good at dealing with issues like this.
(d) I know that I can solve most security problems.
(e) I am easily discouraged by failure.
(f) I don't see the point in trying.
(g) I feel helpless.
(h) They feel like impossible problems.
(i) I have friends/family who can help me deal with the threats.

(j) I have people who can support me while I deal with the issue.
(k) I don't have any technically minded friends who can help me.
(l) I don't have anyone I can turn to for support.
(m) I see them as learning experiences.
(n) The experiences help me learn how to cope under pressure.
(o) I view them as challenges.
(p) I can use the experiences to improve.

Q28. The following guidelines have been obtained in consultation with an online police, the Information System Authority, cybersecurity experts and Smart-ID and Mobile-ID user support. **Which of the following recommendations did you already know before reading it here?** – I knew about it; I knew about it and have used it; First time I hear about it
(a) If someone you know sends you a letter you weren't expecting and asks you to open the attachment or click on a link, then to make sure it's safe, check with them through another channel to see if it were really they who sent it.
(b) If you receive a mail containing a link or attachment sent by someone you do not know, then check the link or attachment in a dedicated virtual environment such as VirusTotal www.virustotal.com.
(c) If you wish to ensure that the visible link and the actual link are the same, hover over the visible link, copy it with right-click, paste it into a text editor and compare it with the visible link.
(d) If your phone displays a different verification code than the webpage you started from when you sign in with Smart ID or Mobile ID, cancel the sign-in, restart your phone and try again. If the codes do not match on the second attempt, inform the Smart-ID or Mobile-ID provider and wait for instructions.
(e) If you suspect someone else is using your name online, or if you have been the victim of bullying or harassment, the best thing to do is to report it to the online police in your area via a contact at www.politsei.ee/et/piirkonnapolitsei.
(f) If you come across a cyber crime (account takeover, ransomware attack, theft of money from a bank account, etc.), report it to the police at cyber.politsei.ee.

Q29. Can you check whether the three links above are safe and lead to the pages they appear to lead?
(a) Yes.
(b) No.

Q30. Did anyone help you respond to this questionnaire?
(a) Yes.
(b) No.

Q31. All my questions are over. If you want to add anything or give feedback, you can do so in this text box.