Vilniaus universiteto leidykla

Contents lists available at Vilnius University Press

Information & Media
2023, vol. 96, pp. 80–94

eISSN 2783-6207
DOI: https://doi.org/10.15388/Im.2023.96.67

Cyber Literacy Skills of Estonians: Activities and Policies For Encouraging Knowledge-Based Cyber Security Attitudes

Kate-Riin Kont

Estonian Academy of Security Sciences, Institute of Internal Affairs
kate-riin.kont@sisekaitse.ee

Abstract. With the advent of COVID-19, people spent more time at home. Countries, societies, companies and individuals suddenly became dependent on cyberspace overnight. Work, shopping and leisure meant we became more than ever weak to the risks of cyberspace. The human factor makes people the "key" to otherwise technically hardly penetrable systems – criminals play on people's greed, emotions, happiness, etc.

It is no surprise that Estonians are more active daily internet users compared to the rest of the Europeans. But what is being done in Estonia at the national level, as well as in cyber protection organisational level, to raise the awareness of residents about cyber security? What else should be done to reduce victims among ordinary citizens and how to protect various important public and private organisations from the consequences of the cyber-risky behaviour of their employees? What is the role of libraries in promoting cyber security awareness? A human error is a central target of cyber attacks, phishing scams, and data breaches. Cyber criminals are becoming more and more inventive. It is important to understand that cyber security risks can be managed and mitigated, but not completely eliminated. Increasing security awareness is the only factor that can help limit breaches caused by human frailty.

Keywords: Cyber security, Cyber security strategies, Cyber literacy, Cyber awareness, Training, Attitudes

Estų kibernetinio raštingumo įgūdžiai. Veikla ir politika, skatinanti žiniomis paremtą požiūrį į kibernetinį saugumą

Santrauka. Prasidėjus COVID-19 pandemijai žmonės daugiau laiko leido namie. Staiga, per naktį, šalys, bendruomenės, įmonės ir asmenys tapo priklausomi nuo kibernetinės erdvės. Dirbdami, apsipirkdami ir leisdami laisvalaikį tapome labiau pažeidžiami kibernetinėje erdvėje. Žmonės dėl žmogiškojo veiksnio tampa „raktu" šiaip jau techniškai sunkiai įveikiamose sistemose – nusikaltėliai naudojasi žmonių godumu, emocijomis, laime ir t. t.

Nenuostabu, kad estai, palyginti su kitais europiečiais, kasdien vis aktyviau naudojasi internetu. Tačiau kaip Estijoje valstybiniu lygmeniu ir kibernetinio saugumo organizacijose lygmeniu yra didinamas gyventojų supratimas apie kibernetinį saugumą? Ką dar reikėtų padaryti, kad sumažėtų nukentėjusiųjų tarp paprastų piliečių, ir kaip apsaugoti įvairias svarbias viešas ir privačias organizacijas nuo jų darbuotojų elgesio, keliančio pavojų kibernetiniam saugumui, pasekmių? Kokį vaidmenį atlieka bibliotekos, skatindamos supratimą apie kibernetinį saugumą? Kibernetinėmis atakomis, duomenų vagystėmis ir duomenų saugumo pažeidimais siekiama žmogaus klaidos. Kibernetiniai nusikaltėliai tampa vis išradingesni. Svarbu suprasti, kad kibernetinio saugumo rizika gali būti valdoma ir švelninama, bet jos visiškai pašalinti negalima. Supratimo apie saugumą didinimas yra vienintelis veiksnys, galintis padėti sumažinti žmogaus pažeidžiamumo sukeltus saugumo pažeidimus.

Received: 2023 02 05. **Accepted:** 2023-04-06.

Pagrindiniai žodžiai: kibernetinis saugumas; kibernetinio saugumo strategijos; kibernetinis raštingumas; supratimas apie kibernetinį saugumą; mokymai; požiūris.

Introduction

Across Europe, the number and sophistication of cyber attacks and cybercrime are increasing. Estonia was already a significantly digitised country in 2007, with good access to the Internet, digital identity cards, 80% of Internet banking, electronic tax collection and a high rate of use of remote medical monitoring. In April 2007, coordinated and large-scale denial-of-service attacks took place against Estonian government infrastructure, financial service providers and domestic media. During the three weeks from April 27 to May 18, 2007, Estonian Internet infrastructure components and websites were attacked, and email inboxes were filled with spam and phishing emails (Schmidt, 2013). While attacks on state servers could be interpreted as a political protest, systematic attacks on commercial structures indicate organised activity against the state, be it called cyber attacks or cyber terrorism. Banks were attacked to paralyse economic activity, and media outlets were attacked to prevent the transmission of information, the daily life of small companies was disrupted by the attacks: email servers, network devices, and web servers were loaded to such an extent that the normal business activities of the companies were disrupted (Randel, 2008). Although these were not the first cyber attacks in Estonia, they turned out to be the most sophisticated and clearly politically motivated attacks, and have also become known as the digital Pearl Harbor. After the attacks, a political discussion about cyber security began in Estonia, and the attack also directed the allies towards coordinated action and cooperation. Since then, Estonia has been at the forefront of the international debate on cyber security and cyber defence (Aaviksoo, 2010), and according to the Cyber Security Strategy 2019–2022, cyber security and safety are now accepted as an integral part of the functioning of the state and economy as well as internal and external security (Majandus- ja Kommunikatsiooniministeerium, 2018, 3).

In Estonia, cybercrime prevention is handled by the Police and Border Guard Board under the administration of the Ministry of the Interior. The national cyber security policy is managed by the Ministry of Economic Affairs and Communications, and the development of the national information system and the resolution of security incidents is organised by the Information System Authority. The Estonian Government has organised several campaigns to increase cyber awareness and developed strategies in which, to a greater or lesser extent, goals have been set to increase the awareness of both residents and organisations about the dangers related to cybercrime and the guides about how to avoid them. Moreover, in the surveys of Estonian public opinion on internal security, cyber security is treated as being among one of the most important issues.

Cyber security components and their management include processes, technologies, and people. Although processes and technologies can be made theoretically secure, their actual security depends on the people who use them. It is said that 83% of cyber security

incidents are caused by human factors (Verizon, 2022). This suggests that the human element remains a prime target for unauthorised access to technological systems (Yeng et al., 2021). In addition, it is important whether people use technology safely and know and follow security rules fully and correctly. Therefore, people can intentionally or unintentionally become a threat to any information security solution, and it is the human factor that is considered the weakest link in information security.

Cyber security is an important field of internal security and thus also belongs to the sphere of interest of cyber scientists. There can never be too much cyber awareness – this is a topic that Government agencies and the strategies they develop and update must constantly and consistently deal with. Cyber education should start early – this is how we raise a cyber-smart generation that can fully enjoy the benefits of the digital world.

My academic background and main research topics are related with library and information science, management science, digital technologies, cyber security, and Internet of Things (IoT). After working for 27 years in different positions in academic libraries, in 2018, I started to work in Tallinn Health Care College as a Senior Lecturer. Since 2014, I am the Head of the Collection Development Committee of the Estonian Librarians' Association. After graduating from Tallinn University, School of Digital Technologies as a Doctor of Philosophy (PhD) in March 2022, I have been working as a cyber security, interoperability and IoT researcher in Estonian Academy of Security Sciences, Institute of Internal affairs.[1]

With this review paper, I would like to explain, what the Estonian Government is doing to promote the cyber hygiene education of its citizens, how the cyber security awareness of population and different focus groups is studied, and how important it is to start cyber education as early as possible in order to raise a cyber-smart new generation.

Cyber security and related concepts

While the word "literacy" alone generally refers to the ability to read and write, when you add the word "cyber" in front of it, the term encompasses much, much more. By definition, cyber literacy is the ability to use computer technologies effectively while understanding the consequences of those actions. It is also important to know where to turn to find reliable and accurate resources in cyberspace. Understanding is the keyword here, as it goes beyond knowing how to use technology and focuses on being aware of your actions. Just as we use money every day and should understand the components of financial literacy, we also need to understand the computers and smart devices we use every day and use that knowledge to protect our data and that of our users, find information faster, avoid phishing, and more. Although by now everyone should have heard about data breaches from the mass media, many have not been able to make their security habits more hygienic, i.e. healthier. This can be due to ignorance, denial or a misunderstanding of their role in data protection.

[1] https://www.etis.ee/CV/Kate-Riin_Kont/eng/

Although the terms "cyber security" and "information security" are often used interchangeably in an unstructured network, the two terms are not entirely analogous. There are two reputable sources which define cyber security. ISO/IEC 27032:2012 which defines information security as the "preservation of the confidentiality, integrity and availability (commonly known as the CIA triangle model) of information in cyber space." The ISACA CSx cybersecurity fundamentals study guide (2016) states that "…but in reality cybersecurity is a part of information security", and

> *"Information security deals with information, regardless of its format–it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications. Cybersecurity, on the other hand, is concerned with protecting digital assets–everything from networks to hardware and information that is processed, stored or transported by internetworked information systems. It is helpful to think of cybersecurity as a component of information security".*

Although not recommended by terminologists, it can be justified by the fact that the term information security describes: "processes and methodologies designed and implemented to protect print, electronic or any other confidential information, private and sensitive information or data from unauthorised access, use, misuse, due to disclosure, destruction, modification or interruption" (SANS Online). Although this definition has some similarities with cyber security, cyber security itself goes a step further by redefining cyberspace (van den Berg et al, 2015). While information security is more focused on the technical side, cyberspace adds two additional layers, a socio-technical layer, in which the technology is controlled by people, and a management layer, in which the cyber aspect must be integrated into the strategic processes of the organisation (de Vries, 2017, 13).

In information security, the reference to the human factor is usually related to the roles of people in the security process. In cyber security, the human factor has an additional dimension, namely people as potential targets of cyber attacks or even unknowing participants in a cyber attack (von Solms & van Niekerk, 2013, 97). Dhillon (2007, 19) also refers to the term data security, which refers to the protection of actual data in an information system. Data security depends to a large extent on the security of the information system where the data resides.

Cyber security awareness of the population

Cybercrime is a critical threat to the European economy, therefore it is considered very important to regularly monitor the cyber security awareness and behaviour of both the population and companies on the Internet. Awareness is the perception of a specific situation or event and a cognitive response to it. Achieving awareness is a multi-step process. The first step is to introduce a concept or fact. This fact is either pushed out of a person's mind or registered as knowledge. The last and most important step in gaining awareness is when that knowledge is used to change attitudes or behaviour. This occurs when a person is finally productively aware of a concept or fact (Srivastava, 2016). Siponen (2000) defined cybersecurity awareness as a methodology to educate internet users to be careful

to the various cyber threats and the vulnerability of computers and data to these threats (Siponen, 2000). Zwilling et al., (2020) pointed out that that hackers tend to seek out the most vulnerable users, i.e. those deficient in information and network security awareness (Zwilling et al., 2020, 2). The most efficient plan to increase cyber security awareness is the improvement of the know-how of the citizens and actors of the economic life and public administration (Letho, 2015).

Eurobarometer surveys

Extensive research on cyber security and cybercrime is being conducted in many parts of the world. Undoubtedly, one of the most comprehensive is the Eurobarometer, with its series of public opinion surveys that compare the dominant attitudes of all EU member states. Estonian respondents have participated in all the studies mentioned below, and from the summary reports of these studies, we can get a very good overview of Estonians' cyber hygiene trends.

Since 2012, a Eurobarometer survey on the attitude of Europeans towards cyber security has been organised regularly. The aim of the survey is to understand EU citizens' awareness, experiences and perceptions of cyber security issues, and the results are compared with previous surveys where possible. The number of respondents is of the same order of magnitude and the methodology is also the same as in previous studies. Each survey report begins by looking at respondents' Internet usage and devices used to access the Internet, and the activities they do online, addressing respondents' concerns about various aspects of online security, including concerns about online banking or online shopping. It also looks at what changes the respondents have made in their cyber behaviour due to concerns about security and privacy, for example, whether passwords have been changed, and whether different passwords are used for each account. A further focus is on respondents' level of awareness of cybercrime risks: how many cyber security issues they know and whether they are concerned about becoming a victim of cybercrime. The discussion then moves on to address the respondents' personal experiences, as well as explore their awareness of other people who have experienced them. Victims of cybercrime are also discussed. Detailed measures taken by respondents to protect children from online harassment are presented. The report concludes by examining respondents' awareness of where they can report cybercrime or illegal online behaviour, as well as the frequency with which these crimes are reported. It also discusses what respondents would do if they were victims of different types of cybercrime.

Internet users have become more aware of the dangers and have changed their cyber behaviour in many ways accordingly. However, it is a cause for concern that in 36 per cent of Internet users in Estonia do not change their online passwords with sufficient regularity, and only about 1/3 use different passwords for different accounts (Europeans' attitudes towards cyber security, 2020).

The Eurobarometer also investigates whether EU citizens have heard anything about cybercrime and how well-informed they feel about the dangers of cybercrime. In most

of Europe, less than half of respondents consider themselves well-informed about the dangers of cybercrime. A growing majority of respondents are concerned about being a victim of, or possibly experiencing, various forms of cybercrime, but few have actually experienced it.

Academic surveys conducted in Estonia

Although mass surveys of the population are important and show trends in the rise of awareness of cyber hygiene or the increase of careless behaviour, the most frequent violations of cyber security requirements are in organisations and are mostly associated with human errors, which can be avoided by regularly assessing and measuring people's cyber hygiene and training them. Cybercrime is a fairly young field of scientific research that has attracted interest in both academic research and practical activity. The ability to exploit human nature relatively easily has created a situation where many attacks focus on the weaknesses of the human factor. It is necessary to raise the awareness of different groups of the population and organisations, and their employees as well as about information security and to promote their ability to deal with unsafe behaviour related to cyber security (Mäses, 2015). In Estonia, the cyber knowledge and cyber hygiene of different groups of the population have been studied for many years.

In 2015, Sten Mäses (2015) for the first time in Estonia tested the knowledge-attitude-behaviour (KAB) model used by Parsons et al. model to determine IT-specialists' cyber awareness. The aim of his work was to present this method, which allows employees to evaluate their information security-related knowledge, attitude and behaviour across different fields. For his master's thesis, Mäses specially developed an interactive web-based test[2] which gives immediate feedback to the test taker, listing his/her estimated strengths and weaknesses. In addition, the employee who has passed the test is shown recommendations for further improvement of security-conscious behaviour. Unfortunately, the test is only in English and cannot be used, for example, to assess the cyber awareness of many employees or the population (Mäses, 2015, 5).

The goals of Alex Bindevald's study "Cyber security in schools – challenges, opportunities and needs for a CTF solution" defended at TUT in 2021 were to find out what is taught in general education schools, and how, within the framework of cyber protection and what extracurricular activities students can use to learn cyber protection. To achieve this goal, the author conducted a survey and an interview with teachers. The results of the survey showed that currently there is a curriculum for teaching cyber security in primary and secondary schools, but since schools themselves can choose what to teach, cyber hygiene is therefore only actively taught in a few schools. In addition to formal education, students can acquire skills related to cyber security from summer camps, training environments and cyber security competitions (Bindevald, 2021, 4).

[2] -https://testing.planet.ee/

Since 2017, the KüberPähkel[3] annual survey aimed at school students has been organised. KüberPähkel is the code name for the survey and testing of primary school, secondary school and vocational school students initiated by the Ministry of Defence and conducted by the Tallinn University of Technology (TalTech) Centre for Cyber Forensics and Cyber Security. The focus is on different knowledge about digital safety and cyber protection, such as: a) privacy and security – what data is reasonable to share on the Internet, and what is not? Where do I have an account and what is a good password? b) technical savvy – do you know what to do before you want to sell your computer? How to lock the screen of a smart device securely? c) cyber defence problem-solving skills – how do you identify what has happened and find solutions? d) behaviour on the Internet – how am I smarter and can I help others when a concern needs to be resolved? How do I identify people with bad intentions? e) problem-solving skills – what to do when things are not as they should be? Can you spot "wrong" things and offer a solution to them?

Surveys of public opinion on internal security conducted in Estonia

Surveys of public opinion on internal security have been conducted at biennial intervals since 2016, and in each survey the cyber security component has become increasingly important. To date, a total of four research reports have been published. In 2016, 44% of Estonian residents saw a cyber attack as the most likely threat out of all threats affecting the entire country, in 2018 only 27%. In 2020, the number increased to 57%, further increasing to 69% of respondents in 2022. In the 2020 and 2022 survey, cyber security is now presented as a separate chapter in the report and includes very detailed questions about how likely it is to be a victim of various types of cybercrime and fraud schemes and whether the respondent has personally fallen victim to situations related to cybercrime in the past 12 months. It also includes what has been done to increase one's cyber security in the last 12 months. In 2020, 58% of respondents considered their awareness of the risks related to cybercrime very good or good, and in 2022, 59% of respondents. Comparing the 2020 and 2022 surveys, all cyber security threats were considered more likely this year compared to the previous survey. In this regard, the following types of cybercrime stand out in particular: access to social media, bank or other personal data by strangers, identity theft and entering one's passwords on fake websites. Respondents who have done nothing to ensure their cyber security were 15% in 2020 and 8% in 2022. Fortunately, there are also only a few who have actually encountered cybercrime. However, of the few who did fall victim in the past 12 months, 71% did not report it to the police or other authorities[4].

[3] https://sites.google.com/view/kyberpahkel/uuringuanal%C3%BC%C3%BCsid

[4] Siseturvalisuse avaliku arvamuse uuring, 2016: aruanne (2016). https://digiriiul.sisekaitse.ee/handle/123456789/2627

Siseturvalisuse avaliku arvamuse uuring, 2018: aruanne (2018). https://digiriiul.sisekaitse.ee/handle/123456789/2623

Siseturvalisuse avaliku arvamuse uuring, 2020: aruanne. (2020). Tallinn: Siseministeerium. https://digiriiul.sisekaitse.ee123456789/2604

Siseturvalisuse avaliku arvamuse uuring, 2022: aruanne (2022). https://digiriiul.sisekaitse.ee/handle/123456789/2604

In the period from 8–21 January 2021, the research company Saar Poll OÜ organised a survey of the Estonian population, with a sample of 1,000 people. The survey revealed that abuse of personal data by cybercriminals, as well as personal data becoming public due to someone's negligence or mistake, are considered the biggest threats. Cyber attacks and cybercrime were most often considered security threats. Foreign information warfare and/or the spread of false information was also considered a big threat (Puusalu & Marnot, 2021, pp. 5–6).

Activities in Estonia to ensuring the cyber security awareness of citicens

Cybercrime is a large and growing problem. One of the target areas for cybercriminals is healthcare. The Information System Authority (RIA) wrote in its 2019 yearbook[5] that cyber incidents in the healthcare sector and leaks of health data are major problems. RIA works to ensure that the healthcare sector can handle information more securely. However, many other organisations, such as libraries and archives, also collect personal data about their users. Furthermore, we can only imagine what would happen if the entire digitised cultural memory of Estonia disappears due to someone's negligence. The current knowledge of cybercrime is mainly based on the study of technical aspects, but as time goes on, more attention has been paid to human factors as well. Several development plans and strategies have been developed in Estonia that emphasize the importance of digital literacy.

Activities and strategies in national level

According to RIA, "since 2007, Estonia has been actively engaged in ensuring cyber security at the national level in order to ensure the safety and availability of state institutions and vital services in any situation" (Vaks, 2013). The *Cyber Security Strategy 2008–2013* was Estonia's first national strategy document that acknowledged the cross-cutting nature of cyber security and the need for coordinated action. It was also one of the first cyber strategies in the world – cyber security and safety were only perceived as an aspect of national security and safety after the cyber attacks against Estonia in 2007 (Majandus- ja Kommunikatsiooniministeerium, 2008).

The *Cyber Security Strategy 2019–2022* (Majandus- ja Kommunikatsiooniministeerium, 2018) was prepared as a single process together with the *Estonian Information Society Development Plan 2020* (Majandus- ja kommunikatsiooniministeerium, 2018) and the *Estonian Lifelong Learning Strategy 2014–2020* (Haridus- ja teadusministeerium, 2014). The first is based on the understanding that to create and develop a successful e-state, the development of the information society and ensuring cyber security must take place at the same time. The goal of cyber security in society is to strengthen resistance to cyber threats and to ensure the conditions for all citizens and entrepreneurs to be able to use reliable and well-functioning ICT opportunities, services and digital tools effec-

[5] https://www.ria.ee/en/media/1502/download

tively and safely. During the implementation of the digital revolution programme of the lifelong learning strategy, the aim was to ensure that the competences related to digital skills also include cyber security, as well as integrating elementary knowledge related to cyber security into the curricula. The goal was the conscious and smart integration of digital opportunities into the learning process and, through this, the development of digital competence (including security-related competences) in the field of general education. The new *Digital Society Development Plan 2030* (Majandus- ja kommunikatsiooniministeerium, 2021) highlights specific connections with the *Internal Security Development Plan 2020–2030* (Siseministeerium, 2020). Identity management is emphasised in both development plans. The *Internal Security Development Plan 2020–2030* sets the goal of creating a reliable, innovative and human-centred identity management. In addition, the need to increase the awareness of both residents and organisations about the dangers of cybercrime and the ways to avoid them is emphasised. In this way, the priority activities established in the Cyber Security Strategy are amplified in both development plans and the safety of cyberspace is increased (Siseministeerium, 2020).

In addition to registering and handling cyber incidents on Estonian computer networks, RIA also supervises information systems used to provide vital services, as well as ensuring security through awareness raising, i.e. organising training for information security managers and regular users of institutions. The Estonian Library Association is a cooperation partner in cyber security campaigns organised by RIA. In the autumn and winter of 2019, RIA organised the awareness campaign "Be IT vigilant!", which continued in 2020. During the follow-up campaign, the focus was on increasing cyber awareness among the Russian-speaking elderly, who are not as well informed about Internet threats. The role of libraries in raising cyber and information security awareness cannot be underestimated. To improve the awareness of librarians, RIA online trainings were held in Tallinn, Harju County and Ida-Viru County. In November and December 2020, a cyber security hotline for the elderly was also opened (Tõiste, 2021). Al-Suqri et al. (2020) have emphasised the role of libraries in an aspect that has not been discussed in Western scientific literature so far – namely, activities in promoting national security and preventing cybercrime. In particular, these activities must ensure that all citizens have access to information and can effectively participate in democratic processes; promote cyber, digital and information literacy to enable library users to critically evaluate and understand information; provide the formation of positive social attitudes and values, and an active role in disseminating information about specific threats to the country's citizens (for example, cyber awareness campaigns, etc.) (Al-Suqri et al., 2020, 22). In the UK, researchers have found evidence of a growing gap between those with and without digital literacy, who are therefore unable to protect themselves online, and highlighted the role of libraries in closing this gap (Clark, 2016). Libraries have been not only cultural centers in countryside areas of Estonia, but also regional centers where residents can receive free digital and cyber literacy training. The closing of libraries is a process that has always reflected what is happening in society. Unfortunately, in 2022, a total of five public libraries were closed in Estonia, this year a decision has been made to close five more libraries.

Activities of different cyber defence organizations

One way to raise awareness of cyber threats and increase awareness of cyber security among different target groups and the population is to organise information days, seminars and competitions. For example, the company CTF TECH[6], which has organised the Cyber Battle of Estonia series of cyber events aimed at young people. The main goal of the competition is to introduce the cyber world to young people who acquire their first knowledge in the cyber field through practical cyber courses. CTF TECH tries to teach young people cyber skills in a computer game-like environment. The aim is to bring as many young people as possible into the cyber field. CTF TECH starts with young people aged 12–13 up to 24 years old. You have to start young to get the young person to take the next step – give them the first cyber experiences in a playful way, teach them to follow cyber hygiene, set secure passwords, etc. In this way, a positive change takes place in young people, and hopefully they will go to university to study this field.

In 2021, the Cyber Pin was held for the first time, which is a mini-test/competition for the secondary schoolchildren in the field of digital threat, cyber security and puzzle.

The annual cyber awareness campaign is coordinated by the European Union Agency for Cybersecurity (ENISA)[7] and supported by the European Commission, EU member states, Europol, the European Central Bank, the European Free Trade Association (EFTA) countries and more than 300 public and private sector partners. The month-long campaign every year in October will introduce up-to-date cyber security tips to boost confidence against internet-based services and support citizens in protecting their personal, financial and work-related data on Internet[8]

Moreover, as an independent international organisation, the NATO Cyber Defense Center (CCDCOE)[9] based in Tallinn, focuses on applied research, analysis, information sharing, and training and exercises in the field of cyber defense. CyCon, the Cyber Defense Center's annual conference, brings more than half a thousand experts from all over the world to Tallinn every spring, representing governments, defence forces, private companies, universities, etc. This is a multidisciplinary conference, introducing keynotes and panels focusing on the technical, legal, policy, strategy and military perspectives of cyber defence and security. Various, mainly technical trainings are organized, but only in English. CCDCOE has also an e-library[10] wich includes e-books, articles, reports and videos in focus areas. The trainings[11] and exercises[12] are also available.

On 30 September 2022, the seminar "The Role of Libraries in Creating a Safer Cyberspace" was organised by the Internal Security Institute of the Estonian Academy of Security Sciences. The seminar gave the knowledge that cyber topics are not only a matter for cyber specialists.

---

6 https://www.ctftech.com/
7 https://www.enisa.europa.eu/
8 https://cybersecuritymonth.eu/
9 https://ccdcoe.org/
10 https://ccdcoe.org/library/publications/
11 https://ccdcoe.org/training/
12 https://ccdcoe.org/exercises/

There is also Security Education and Training Awareness (SETA) Toolkit[13] which is important because it does not only contribute to safer usages at work (Barlow et al., 2016; Dhillon et al., 2020; Yoo et al., 2018) but also to the overall population awareness of information security issues. E.g. D'Arcy et al. argue that security education, training and awareness programs ("SETA programs") are necessary to prevent the misuse of information systems (D'Arcy et al., 2009). However, Grassegger and Nedbal (2020) rejected the hyphothesis that SETA programs have a positive impact on the information security awareness of employees, it was not supported by their study (Grassegger & Nedbal, 2020).

Thus, we can say that residents, managers and employees of all organisations in Estonia must be by now more aware of the dangers of cybercrime, which is becoming more and more complex. Therefore, why we still hear and read the news, that "Latvian citizens 'donated' to cybercriminals 12m in 2022" or "Last week, the police received a crime report from a woman from Tallinn who had transferred over 60,000 euros to a man who promised to marry her, but the good life and wedding did not happen"?

Discussion and solutions

The avalanche of cyber fraud shows no sign of abating. The results of Eurobarometer surveys show that Internet users have become increasingly aware of the dangers with each study and have changed their cyber behaviour. However, all this shows that we need to go deeper with the cyber literacy trainings and surveys. In addition to population surveys, we need to find those target groups that are most vulnerable to cyber attacks - for example, cyber bullying among children and young people, women falling victim to fraudsters in social networks on their way to search of a dream partner, or the elderly, who easily fall victim to provocations and hand over their bank account PIN codes, etc. We cannot recommend to these people to participate in CCDCOE conferences or reading materials from CCDCOE e-Library and train themselves via SETA. The reason is that the conferences of the CCDCOE and the electronic materials available in the e-library are all in English, and therefore do not fulfill the purpose of raising the cyber awareness of the population. Also SETA cannot be recommended to train the ordinary citicens because the English language skills among middle-aged and senior citizens is above the level to understand the materials. However, it can be helpful for public and private organisations to raise the awareness of their employees.

Therefore, despite several organisations focused on cyber security and defense in Estonia, and seemingly excellent training materials in English, the question remains *How to reduce victims among ordinary citizens from the consequences of the cyber-risky behaviour or non-awareness?*

First, the cyber awareness of these groups must be studied to identify their weak points, because also the questionnaire study can be the tool for raising awareness – people start to think about issues which they have not paid attention to before, then training plans or

[13] https://www.cdse.edu/Training/Toolkits/Security-Education-and-Training-Awareness-Toolkit/

campaigns must be developed. After the training or campaign, a new survey should be conducted to find out whether the awareness increased as a result. E.g., two campaigns against cyberbullying have taken place in Estonia – in 2017 and in 2023. However, there are no measurements of the 2017 campaign aftereffect to make conclusions was the campaign successful or not.

As a result of this study, it can be stated that there is a need to increase the awareness of the population about cyber threats, including cyber attacks and cybercrime, and about mitigating/preventing threats to personal data. The assessment of awareness shows that the population's knowledge of the use of data and having control over it is low. Although the aim of the *Lifelong Learning Strategy 2014–2020* was to ensure that competences related to digital skills also include cyber literacy and that in addition to digital technology, elementary knowledge related to cyber security is also integrated into the curricula, Alex Bindevald's research showed that, although there is an optional subject for teaching cyber security in primary and secondary schools, cyber hygiene is actually only taught in a few schools. However, there is a strong need to strengthen all strategies developed at the national level. At the moment, several strategies have been developed in Estonia, an important part of which is raising cyber awareness. Unfortunately, not everything planned in the strategies has been implemented.

Raising awareness and introducing and maintaining good usage habits to mitigate risks requires additional and continuous information and training activities. Starting to teach cybersmart generation to integrating cyber security as a compulsory subject into the curriculum of high schools is extremely important in order to ensure the future growth of cyber-aware citizens.

Future Talks

Surveys of the population's awareness of cybercrime have been conducted in Europe and Estonia for more than ten years. Although, according to experts, it will never be possible to completely eliminate cybercrime and prevent cyber attacks, training employees of organisations and different groups of the population, and constantly monitoring their cyber awareness – cyber security knowledge, attitudes, skills and actual behaviour – is increasingly important. The results of Eurobarometer surveys, the results of internal security public surveys and the RIA data show that the cyber hygiene habits of the people of the EU and Estonia are improving, but not as fast as can be expected.

Unfortunately, there is still a large number of people who do not know how to use computers and smart devices very well, and do not know how to navigate the ever-increasing amount of information. The government has the responsibility to train such people, e.g. using the help of local libraries, etc. National strategies are written with the aim that they can be applied in real life and not just remain on paper. There is currently room for improvement. Activities in promoting national security and preventing cybercrime must ensure that all citizens have access to information and can effectively participate in democratic processes; promote cyber, digital and information literacy to enable citizens to critically

evaluate and understand information. In the UK, researchers have found evidence of a growing gap between those with and without digital literacy, who are therefore unable to protect themselves online (Clark, 2016). Cyber security should already be integrated into the curriculum of upper secondary schools, thus creating the prerequisites for the generation of cyber-aware citizens through the formal education system. These same young cyber-smart people could share their experiences and teach the older generation. This topic could be covered, for example, in TV shows intended for the elderly, etc. That way we could all enjoy the digital life.

References

Aaviksoo, J. (2010). Cyberattacks Against Estonia Raised Awareness of Cyberthreats. *Defence Against Terrorism Review*, 3(2), 13–22. https://www.coedat.nato.int/publication/datr/volumes/datr6.pdf

Al-Suqri, M. N., Alkindi, S. S., Saleem, N. E., Al-Nabhani, M. S. & Fadhil, B. S. (2020). Libraries and National Security: A Review of Evidence and a Proposed New Strategic Direction. *Journal of Arts & Social Sciences*, 11(3), 17-27. https://journals.squ.edu.om/index.php/jass/article/view/4479/3264

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Barlow, J.B., Warkentin, M., Ormond, D., & Dennis, A. (2018) Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, 19(8), https://doi.org/689-715. 10.17705/1jais.00506

van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boekee, S., Koppen, L., van den Berg, B., A de Bos, A. & van der Lubbe, J.C.A. (2015). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. In E. Luijff, E.(Ed.), Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium, Tallinn, Estonia, October 13-14 2014 (pp 1-10). NATO Science and Technology Organization.

Bindevald, A. (2021). Küberturvalisus koolides - väljakutsed, võimalused ja vajadused CTF-lahenduse järele. Cyber Security at Schools - Challenges, Opportunities and Needs for CTF-Solution. Tallinna Tehnikaülikool. https://digikogu.taltech.ee/et/Item/49f9674f-34c7-4db6-a938-25738dd2d61f

Clark, I. (2016). The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2, 1-32. https://journal.radicallibrarianship.org/index.php/journal/article/view/12

Dhillon G., (2007). Principles of information systems security. John Wiley & Sons.

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions. Journal of the Association for Information Systems, 21(1), 152-174. https://doi.org/10.17705/1jais.00595

Europeans' attitudes towards cyber security (cybercrime) - Publication Reports. Special Eurobarometer 499. (2020). https://europa.eu/eurobarometer/surveys/detail/2249

Grassegger, T. & Nedbal, D. (2020). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*, 181, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Haridus- ja teadusministeerium. *Eesti Elukestva õppe strateegia 2020.* (2014). https://www.haridusfoorum.ee/images/haridusstrateegia/Eesti_elukestva_oppe_strateegia_loplik.pdf

ISACA (2016). ISACA CSx Cybersecurity Fundamentals Study Guide. https://1filedownload.com/cybersecurity-fundamentals-cybersecurity-nexus-cissp-study-guide/

ISO (2012), ISO/IEC 27032:2012 (Information technology – Security techniques – Guidelines for cybersecurity). https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Lehto M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS 2015; 2015 Jul 1; Hatfield (UK): University of Hertfordshire, Academic Conferences and Publishing International Limited, (pp. 179–88). https://jyx.jyu.fi/bitstream/handle/123456789/46540/lehtoeccws2015.pdf?sequence=1

Majandus- ja kommunikatsiooniministeerium. *Digiühiskonna arengukava 2030.* (2021). https://www.mkm.ee/media/6791/download

Majandus- ja kommunikatsiooniministeerium. *Eesti infoühiskonna arengukava rakendusplaan 2018-2022.* (2018).

Majandus- ja Kommunikatsiooniministeerium. *Küberjulgeoleku strateegia 2008–2013*. (2008) https://energiatalgud.ee/sites/default/files/images_sala/e/ea/Kaitseministeerium._K%C3%BCberjulgeoleku_strateegia_2008_-_2013._Tallinn_2008.pdf

Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse strateegia 2019–2022*. (2018). https://www.mkm.ee/media/700/download

Mulwad, V., Li, W., Joshi, A., Finin, T. & Viswanathan, K. (2011). Extracting Information about Security Vulnerabilities from Web Text. In Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Lyon, France, 22 August 2011 (3), 257–260. https://doi.org/10.1109/WI-IAT.2011.26

Mäses, S. (2015). Infoturbe inimfaktori hindamismeetod. Evaluation Method for Human Aspects in Information Security. Tallinna Tehnikaülikool. https://digikogu.taltech.ee/et/Item/1c19ddce-e325-440c-838f-9a349e087ca6

Puusalu, J. & Marnot, D. (2021). Elanikkonnaküsitlus „Eesti elanike suhtumine isiklike andmete privaatsusesse ja turvalisusesse“. https://digiriiul.sisekaitse.ee/handle/123456789/2846

Randel, T. (2008). CERT Eesti tegevuse aastakokkuvõte 2007. https://www.ria.ee/media/1532/download

SANS. Information Security Resources Online. https://www.sans.org/information-security/

Schmidt, A. (2013). The Estonian Cyberattacks. In J. Healey (Ed.). The fierce domain – conflicts in cyberspace 1986–2012. Atlantic Council. https://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8(1), 31-41. https://doi.org/10.1108/09685220010371394

Siseministeerium. *Siseturvalisuse arengukava 2020–2030*. (2020). https://www.siseministeerium.ee/media/748/download

Rossouw von Solms, R. & Johan van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

von Solms, B. & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Srivastava, A. (2016). Awareness Surveys: The Data-Driven Way to Read People's Minds. https://humansofdata.atlan.com/2016/04/awareness-surveys-read-peoples-minds/

Tõiste, T. (2021). Eesti Raamatukoguhoidjate Ühingu tegevus 2020. aastal. https://eru.lib.ee/images/stories/dokumendid/ERY_2020_aruanne.pdf

Vaks, T. (2013). Riigi Infosüsteemi Ameti kokkuvõte küberturvalisuse tagamisest 2012.

Verizon. (2022). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

de Vries, R. (2017). A methodology for quantifying the level of cybersecurity awareness. Leiden University. https://studenttheses.universiteitleiden.nl/access/item%3A2666282/view

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Hamdullah, N.B. (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-90. https://doi.org/10.1080/08874417.2020.1712269

Yeng, P. K., Fauszi, M. A. & Yang. B. (2021). Assessing the effect of human factors in healthcare cyber security practice: An empirical study. 25th Pan-Hellenic Conference on Informatics. November 2021. Pages 472–476. https://doi.org/10.1145/3503823.3503909

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. Decision Support Systems, 108, 107-118. https://doi.org/10.1016/j.dss.2018.02.009