Baltic J. Modern Computing, Vol. 13 (2025), No. 2, 502-527
https://doi.org/10.22364/bjmc.2025.13.2.11

Cyber Threat Risks in Higher Education Institutions: an Example of the Estonian Academy of Security Sciences

Kate-Riin KONT

Estonian Academy of Security Sciences, Internal Secyrity Institute, Kase 61, 12012 Tallinn, Estonia

kate-riin.kont@sisekaitse.ee

ORCID 0000-0002-9184-2363

Abstract. Purpose of this study is to identify the most common characteristics that make users vulnerable, either individually or in groups, and to determine whether there is a relationship between user behaviour and victimisation of a cyber-attack. This research should help characterise people who are more likely to become victims of various phishing and social attacks. For this purpose, students, employees and lecturers of the Estonian Academy of Security Sciences were investigated. A five-scale questionnaire was used as the methodology of the study, which takes into account the following behaviour scales: risky behaviour, conservative behaviour, risk exposure behaviour and risk perception behaviour. Survey scales already used in previous studies were applied to the students, academics and administrative staff of the Estonian Academy of Security Sciences (hereinafter Academy). These scales and questions are quite well suited for identifying cyber risks that are threatening the patrons of higher education institutions. The results of the study show there are significant differences within the samples and according to Internet usage habits and positions in the Academy.

Keywords: Cyber security, Cyber threats, Higher Education Institution, User behaviour, Risky behaviour, Conservative behaviour, Exposure behaviour, Risk perception behaviour

1. Introduction

The use of digital technologies in the education sector has increased worldwide in recent decades. Educational technologies have become an integral part of teaching and learning processes in the form of computer devices for content delivery, online learning applications, cloud storage, learning management systems, and computer-based assessment and training systems. Especially after the COVID-19 pandemic, many educational institutions have no choice but to use distance learning with the help of digital technologies to ensure the continuation of teaching. However, the increasing use of technology in education brings with it a number of challenges, including technical and human behavioural issues of cyber security, and insufficient cyber training for faculty, staff and students. In recent years, several cyber incidents against higher education institutions have exposed the problems that cyber threats can bring to educational

institutions. These incidents have resulted in large-scale personal data leaks of students, staff and alumni, and ransomware attacks, which also cause serious financial losses, in which the target is blocked from accessing their data and a ransom is required to regain access or prevent data leakage. (Noran, 2021).

Cyber security means that digital data and the processing of that data are fully protected. Data creation, transmission, storage, presentation and all other data handling processes are protected. In other words, cyber security is a state where all kinds of threats that could affect digital data and the use of computers, smart devices, memory sticks and e-services do not materialise. In cyber and information security, there is a question about security. Safety is a subjective experience, there is no unequivocal description of safety. Everyone also experiences security in their own way: the same security threat can cause a much stronger feeling of insecurity in one person than in another. Security is made up of several factors: emotion, learned patterns, reality, and our ability to withstand disturbances and crisis situations. Security is an emotional state that varies depending on the situation a person is experiencing. Reality is an important factor in security, the way things around us are said to be "cold facts". Learned values and patterns guide people as they value and prioritise safety. Resilience to disruption and crisis situations determine how people respond to disruption. With a good tolerance, one can deal with disturbances without panic. Understanding reality is a priority so that our sense of security is not based on false assumptions. Only with a proper understanding of reality can resilience be strengthened and models that develop safety be created. Our emotions are constantly appealed to in the media, by creating emotions one can influence people well. It does not matter whether our perceptions and fears are based on imaginary or real threats, either way, perceptions and fears drive our behaviour and greatly affect our well-being. To increase safety, development must take place in safety areas (Limnéll et al., 2014).

Although the hardware and software solutions used to ensure cyber security are constantly updated, it is still not possible to prevent information systems from becoming compromised, and the reason for this is precisely the behaviour caused by people's ignorance. Although individuals may have knowledge about cyber security, this knowledge is not always reflected in appropriate behaviour. So, everyday cyber security is not a problem that can be solved by technological solutions alone. People's behaviour in the field of cyber security must be evaluated as the weakest link.

This article is based slightly on a conference presentation given at the CYBER 2023: The Eighth International Conference on Cyber-Technologies and Cyber-Systems conference (Kont, 2023). The study examines the behaviour of students, lecturers (researchers) and employees of the Academy regarding hybrid threats and possibilities to prevent risks related to cyber security. This study is part of a larger research conducted within the framework of the cooperation programme on hybrid threats (HYBRIDC). The results of the study can be used to develop strategies and training to reduce errors related to the human factor in the cyber security of higher education institutions. Based on the two main studies, Ög˘ütçü et al. (2016) and Benavides-Astudillo et al. (2022) of the Risky Behaviour Scale (RBS), the Conservative Behaviour Scale (CBS), the Exposure to Offence Scale (EOS) and the Risk Perception Scale (RPS), this study definitely aimed to obtain answers to the following questions:

- Is there a significant difference between the surveyed groups (females and males) concerning their average score according to different behavioural scales (RBS, CBS, EOS, RPS)?
- Is there a significant difference between the surveyed groups (students, academics and administrative staff) concerning their average score according to different behavioural scales (RBS, CBS, EOS, RPS)?
- Does the duration of time spent on the Internet affect the average of the scales (RBS, CBS, EOS, RPS)?
- Does the cyber security training attendance or non-attendance affect the average of the scales (RBS, CBS, EOS, RPS)?

The results were analysed using SPSS descriptive statistics analysis and ANOVA analysis with post-hoc tests to answer research questions, and the results are presented as tables. The results of the study can be used by either organisations or educational institutions to develop personalised and proactive training programmes or to prepare preventive strategies. This paper is structured as follows. In the literature review section, a brief overview of how a threat is conceptualised in cyber security is given, and an analysis of why security breaches in higher education institutions have become very frequent. In the research methodology section, the author briefly introduces the study design and sample characteristics. The results section answers the research questions. Finally, conclusions are given.

2. Literature review

2.1. Why are higher education institutions the targets of cyber-attacks?

Cyber security in a higher education institution is completely different than in the private sector because it is an open institution. There are many access points, there is a lot of personal information about employees and students. Information security training, awareness raising and cyber behaviour monitoring are not always top priorities for educational institutions. The contribution of lecturers, researchers and employees who engage in research and teaching work or provide administrative support to these activities are often considered to be the central figures of a higher education institution. IT employees deal with security to the extent that they have the human and time resources for it.

Higher education and academic institutions have become beneficial targets for cyber-attackers. In recent years, security breaches in higher education institutions have become very frequent. For example, the University of Maryland has repeatedly been the victim of cyber-attacks – in 2014, over 309,000 personal data records containing social security numbers, dates of birth and university ID numbers were breached. In 2015, the personal information of 288,000 students, faculty and staff at the University of Maryland was breached, and a month later it was breached again (Svitek and Anderson, 2014; Roman, 2018). The University of Maryland was also included in the list of recent actions by Russian hackers (Yerby and Floyd, 2018).

Attempts have also been made in Estonia to gain access to university emails with phishing letters. It was malware hidden in fake emails, which would have given access to the

contents of the email account when activated. For example, in 2020, such an attack was made on the University of Tartu. In this case, too, it was most likely a campaign of Iranian state origin, known as Silent Librarian and Mabna Institute. With its expert action, the university was able to both detect the attack and prevent more damage (Einmann, 2020). On 4 September 2020, Tartu Health Care College was hit by a cyber-attack, which paralysed the use of the institution's service servers for several days. As a result of the break-in, backup copies, clones created for installing workstations, software installation files, the school's image bank accumulated over time and the original material of many educational videos were destroyed after resetting the data repositories (Karu, 2020).

Cyber-attacks on universities show that such an attack can be not only detrimental to relations between countries, but even life-threatening. Düsseldorf University Hospital failed to admit a woman brought by ambulance on 19 September 2020 after a cyber-attack froze the hospital's information system – the prosecutor started a murder investigation. It was the first time a human death was directly linked to a cyber-attack. However, it was not certain if the university hospital was the actual target of the attack or if it was collateral damage in an attack on the university. The ransom demands were aimed at Heinrich Heine University, not the hospital directly connected to it. The police contacted the attackers and informed them that the target of the attack was the hospital, not the university, and that the patient's life was in danger. After that, the attack was stopped and the authorities were given the encryption key, but it was too late (Busvine and Kaeckenhoff, 2020).

The world has been in a new security situation since 2022 when Russia started a war of aggression in Ukraine. Seppänen (2022) emphasises that "Typical information security threats for higher education institutions are phishing attacks and frauds, the aim of which is to obtain user IDs, gain access to higher education systems, or obtain, for example, financial benefits. The resulting data can be used, for example, to deliver scams and phishing messages, as emails sent on behalf of the university are generally considered trustworthy. Every month, hundreds of thousands of phishing messages are sent to individual universities, most of which do not pass technical security measures and are therefore not visible to students." However, in the home office, doing business with one's own devices can transfer information security threats from the private place to the workplace. Data security must be considered as a whole – it does not end when you leave the workplace or close the work laptop, but also in your free time (Seppänen, 2022).

Academic institutions are undertaking more cyber security research than before, while the higher education sector itself often leaves the issue of cyber security to IT technicians. The education sector has proven to be an interesting and, unfortunately, easy target for cyber-attacks. Prevention, collaboration, access rights management and training are examples of safeguards. Higher education often experiences the scenarios described above. Organisations that do not adequately protect and educate themselves may inadvertently expose the personal data of students and staff, as well as research data that is valuable to cybercriminals operating both domestically and internationally. Incidents like these are not stopping, so it is critical for higher education institutions to consider whether their cyber defence management is strong enough.

2.2. What is a cyber threat?

Threat orientation is emphasised in the cyber environment. This means that there is no

security without threats and risks. The threat consists of stability and credibility. In a cyber environment, not all threats can be anticipated or taken into account. Threats like this have come to be called black swans (Limnéll et al., 2014). A cyber threat is an event in cyberspace that can potentially cause a loss of assets and undesirable consequences as a result (Bederna and Szadeczky, 2020). According to Shad (2019), it is the "action that may result in unauthorised access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system" (Shad, 2019). A cyber threat is the possibility of a malicious act, the purpose of which is to damage or disrupt an information network system (Oxford Dictionary, 2019). Threats can be viewed at different levels (international, national, companies and individuals) and their significance varies by level (Iiskola, 2019).

From the state's point of view, the most serious cyber threats are directed at critical infrastructure. The background of the threat may be terrorism, crime, a state actor or a state-sponsored actor. States may use, for example, criminal organisations to achieve their own goals, in which case the actions and the state's involvement are also debatable (Iiskola, 2019). The threats can be classified as enabled by the cyber environment as part of hybrid influence. Hybrid influence is the non-military means of a state actor to influence another state's political and economic decision-making. For example, political opinion may be influenced via social media. In terms of the functioning of society, significant cyber threats are threats to communication services and networks, because the functioning of electricity networks and payment traffic, for example, depend on the functioning of communication services. The most common disruptions in communication services are caused by disruptions in electricity supply. The most serious cyber threat is attacks on energy production and health services due to the potential loss of human lives. Other serious threats are the automation and control systems of power plants or nuclear power plants, food transport and logistics systems, healthcare information systems, traffic control systems, banking and payment systems, and information systems enabling communication services as well as interference with satellite positioning and domain name services. Attacks on critical infrastructure may be attractive because of their effectiveness. Most of the critical infrastructure is held by private companies and organisations. Thus, national-level cyber security cannot be completely separated from corporate and organisational cyber security (Kansallinen riskiarvio, 2024).

Threats to the organisation consist of internal and external threats. External threats can be thought of as a deliberate and purposeful attack by someone outside the organisation. Internal threats can be divided into intentional and unintentional threats. Unintentional threats may be caused, for example, by ignorance, distraction or carelessness. They can also be conscious or unconscious (Limnéll et al., 2014). Intentional internal threats consist of insider crimes. Insider crime refers to a crime committed by a person who is able to utilise information and skills obtained from the organisation that others would not necessarily have had access to. Cyber-attacks by insiders accounted for about 14% of all attacks in 2013. In half of these attacks, the former employee used their old credentials or backdoors that had not been closed (Widup, 2013). In 2018, an insider was involved in 28% of attacks (Widup, 2018). It may be more difficult to protect against an attack by an insider. However, the threat is real, and its importance seems to be growing.

Opportunities also come with risks (Juvonen et al., 2014). According to Hubbard (2020), "Risk means a state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome or event" (Hubbard, 2020). On the other hand, risk can be understood as the courage to make a decision and the freedom to choose between different options. Risks are perceived as scary when they cannot be controlled (Kuusela, 2005). Cyber risk is the risk of financial or reputational loss due to the non-functioning of information technology. Risks are included in all activities and cannot be completely eliminated, unlike threats. Risk is a condition of existence and the possibility of a negative event in the future. However, one can learn to live with risks and manage them. The aim of risk management is to minimise the probabilities and effects of risks. It is a method that aims to identify and assess risks and to choose, develop and implement alternatives. Risk management can also be seen as giving information about the organisation's reliability and responsibility. As a result of successful risk management, resources can be effectively allocated to risk reduction (Limnéll et al., 2014). Technology also increases the possibilities of risk management. However, as addictions increase, the severity and impact of the risks may increase (Kuusela, 2005).

Cyber security is a balancing act between opportunities and threats. Threats are often emphasised in the phenomenon, when opportunities should be emphasised. There is no perfect cyber security, just as there is no perfect physical security either. The best way to prepare for threats is to put the basics in order (Limnéll et al., 2014).

2.3. Factors influencing cyber security and risk behaviour

As educational environments increasingly rely on digital platforms, understanding the factors that influence cyber security practices has become paramount. There are undoubtedly many factors that influence risk behaviour, of which this study focuses on status and gender differences, time spent online, and cyber training.

The assessment of cyber security awareness among students has revealed concerning trends regarding their engagement with protective measures. For instance, Saeed's study indicates that while students demonstrate a reasonable level of awareness regarding cyber security threats, their actual protective behaviors often fall short (Saeed, 2023). This gap between awareness and action highlights the need for targeted interventions that not only inform but also motivate individuals to adopt safer online practices. The implications of these findings extend beyond individual behavior to encompass broader institutional responsibilities. As highlighted by Triplett, educational institutions must proactively address cyber security challenges by implementing strategies that enhance awareness and encourage students to consider careers in cyber security (Triplett, 2023). Similarly, Concepcion's assessment of cyber security awareness among academic employees highlights the necessity of promoting cyber hygiene to secure sensitive information within educational institutions (Concepcion and Palaoag, 2024).

Cyber security awareness and training is a non-technical cyber risk prevention measure organisations use to strengthen the resilience of the socio-technical system at the human factor level (Pollini et al., 2022). Organisational cyber security programmes have traditionally focused on technical controls to protect infrastructure and equipment, while cybercriminals have focused on exploiting human vulnerabilities. Most internal users put the organisation at risk through negligence, error, or lack of knowledge. These non-

malicious actions cause the majority of cyber incidents (Zimmermann and Renaud, 2019). Although employees are mostly informed about cyber risks and measures to mitigate them, it is common for them to take risky actions either out of haste, carelessness or fatigue. Awareness of the cyber risk landscape and the organisation's security policy, along with training on the actions and behaviours needed to mitigate risks, is essential to reduce human error and intentional misuse of information systems, including insider threats to organisations (Hadlington, 2018). Therefore, to mitigate cyber risks effectively, cyber security training has focused on raising awareness and educating end users about cyber risks (Jalali et al., 2019). Qashqari et al. (2020) argue that even with a strong security policy, people are considered the weakest link in information security, therefore, the study of human behaviour from a cyber security perspective is an important topic for organisations. Recent studies have identified that demographics are important factors that influence a person's attitude and behaviour towards cyber security. For organisations to develop effective cyber security training programmes, it is important to understand the security behaviours, similarities, and differences in the behaviour of different target groups.

Anwar et al. (2017) explain that gender is one of the most fundamental social groups that influences an individual's perceptions, attitudes, and outcomes, regardless of whether they are male or female. According to Ifinedo (2012), men have lower rates of security policy compliance compared to women, and the author recommends that those responsible for security and policy pay attention to gender differences in security policy compliance in organisations. The author also calls for the implementation of targeted security awareness programmes, training, and monitoring to eliminate differences in security behaviours between men and women. Verkijika (2019) suggests that women often have lower safety characteristics and related experiences compared to men.

The relationship between time spent online and risk behaviour has been poorly studied. Jeske and Van Schaik (2017) conducted a study on students' awareness of various online threats. Participants were presented with definitions of threats and asked how familiar they were with these threats. The responses showed that time spent online and length of online experience predicted awareness of online threats, which in turn predicted the use of computer security. Average time spent online positively predicted familiarity with threats, as did the duration of Internet use over several years. Familiarity was a significant predictor of positive cyber behaviour. Mediation analysis of the results showed a significant indirect effect, with time spent online and duration of Internet use fully mediating the relationship between awareness of threats and online behaviour. The study provided further evidence that time spent online and length of online experience (although not daily or weekly frequency of use) were significant predictors of threat awareness and online behaviour. These variables were also significant indirect predictors of computer security use, which was fully mediated by familiarity. Although the effects were generally quite small, the practical conclusion can be that computer security behaviour depends on familiarity, which is not achieved without a significant investment of time. This means that the time spent becoming aware of threats and learning about online opportunities is a time of learning, but at the same time a time of increased vulnerability until a certain level of familiarity with threats is achieved, which in turn triggers security behaviour. Duman (2022) studied the impact of students' daily Internet use on cyber security behaviour. The results showed that students' cyber security behaviour differs depending on the time spent

online. Namely, students with lower daily Internet use (less than 1 hour or 1–2 hours per day) had significantly less risky cyber security behaviour compared to students who used the Internet for 3–4 hours or 5 hours per day or more. Based on this result, it can be concluded that students with lower daily Internet use have higher cyber security awareness. However, a similar study by Yiğiti and Seferoğlu (2019) did not find a significant relationship between students' cyber security behaviour and time spent online.

In conclusion, cyber security awareness and training are important measures in organisations to prevent cyber risks, as cybercriminals can often exploit people's vulnerabilities. Recent research underscores the multifaceted nature of cyber security risky behavior factors among students and staff in higher education institutions. The interplay of awareness, individual behaviors, institutional strategies, and social dynamics plays a crucial role in shaping cyber security practices. Based on the reviewed literature, it can be argued that gender differences play an important role in security behaviour – studies have found that men often have lower rates of compliance with security policies than women. The relationship between time spent online and cyber security risky behaviour has also been studied. Studies have shown that longer experience and time using the Internet are associated with greater awareness of risks and online behaviour. However, there are also studies that did not find a significant relationship between Internet use and more secure cyber behaviour.

3. Research methodology, the analysis techniques used and sample characterisation

The Academy was selected for this study primarily because the author is affiliated with the university. As Academy educates future professionals in internal security and operates under the direct supervision of the Estonian Ministry of the Interior, it is expected that both students and staff have received comprehensive training in cyber security. Therefore, it is both relevant and appropriate to assess the cyber security practices of Academy members (students and employees) in their online activities, exploring whether their behavior tends to be cautious or risky. This is the first study on information and cyber security behavior conducted at a higher education institution in Estonia, and its findings may provide insights into the online practices of individuals at other universities across the country.

This research uses a four-scale model to measure behaviour and awareness of cyber security. The Risky Behaviour Scale (RBS) measures the degree of risk of users of information systems related to behaviour, the Conservative Behaviour Scale (CBS) measures how careful users are when using information systems, the Exposure to Offence Scale (EOS) measures users' exposure to cyber security incidents due to their behaviour and the Risk Perception Scale (RPS) measures the level of danger or risk associated with information technology model and survey method to collect data (Benavides-Astudillo et al., 2022; Ceran, 2021; Ög˘ütçü et al., 2016). Using the given model of scales, the challenges of the questionnaire survey were finding out the respondents' attitude towards the survey, successful and comprehensible wording of the answer options, clarity of the scale, and time required to answer the survey (Hirsijärvi, 2010). A major challenge of this study was the possible low response rate due to the novelty of the survey topic. Placing

the questions in the context of Estonian higher education created challenges, as the topic is relatively unaddressed in higher education in the Baltic countries, so there was a high risk of misunderstandings. A questionnaire technique was used to achieve the objectives of the study and the survey was conducted online to obtain a large sample of both staff and students as efficiently and ethically as possible. The questionnaire consisted of 56 questions covering various aspects of cyber security, including the RBS (20 questions); the CBS (10 questions); the EOS (7 questions) and the RPS (17 questions). Additionally, 6 demographic questions were asked, and the questionnaire ended with a so-called open question, where the respondents were asked to express an opinion about the discussed topic or the questionnaire or simply leave a comment. The survey questions were selected based on instruments developed by other cyber security researchers (mainly based on Benavides-Astudillo et al. (2022), and IT-experts-suggested questions from the Academy. The digital team of the Academy added several suggestions to change the wording and order of the questions to make them more suitable for the context of the field of internal security. At the beginning of the questionnaire, the importance of cyber security in higher education was introduced and it was explained why higher education institutions have become attractive and important targets for cybercriminals. The significance and novelty of the questionnaire in the context of both Estonia and the Baltic states were also explained.

Answers were given according to a 5-point Likert type. The proposed scales were formulated depending on the questions asked. Total respondent scores were calculated by assigning 5 points for “Always”, 4 points for “Often”, 3 points for “Sometimes”, 2 points for “Rarely”, and 1 point for “Never” for the RBS and CBS questions. A higher score indicates that the respondent is very risk-tolerant. In RPS, “Very dangerous” is 5 points, “Dangerous” is 4 points, “Slightly dangerous” is 3 points, “Not dangerous” is 2 points and “I don’t know” is 1 point. As the scores increase, it is understandable that the respondent considers related technologies more dangerous (Benavides-Astudillo et al., 2022; Ceran, 2021; Öğ˘ütçü et al., 2016). In EOS, it is said that as the scores increase, the respondent is exposed to crime (negative experience) at a higher level. This was the bottleneck of the EOS scale of the questionnaire, which could not be adapted to the Academy questionnaire with the same points as in the other studies discussed. Since people who are very aware of cyber security and work at the Academy, the majority of them had never or rarely encountered the dangerous cyber situations mentioned in the questionnaire. Therefore, the author decided to invert this scale – 1 point for “Always”, 2 points for “Often”, 3 points for “Sometimes”, 4 points for “Rarely”, and 5 points for “Never” (see desciptive statistics Kont, 2024, pp. 94, 96, 97, 98).

As pointed out in the introduction section, several analysis techniques and tests were conducted to answer the research questions. The analysis of variance (ANOVA) is the most important of these tests and involves an additional post-hoc Tukey test. The meaning of ANOVA can be explained in several ways. First, as a comparison task, i.e. the study of how uniform the averages of groups are under a certain classification. Second, ANOVA as a prediction task, i.e. the study of how well the average variability of the characteristic under study can be described statistically through group membership in a certain classification. This means modelling the relationship between traits and the task of forecasting group means within the model. Variance analysis also makes it possible to deal with classifications based on several characteristics at the same time and in their mutual

interaction, i.e. interaction. The average differences between women and men, the average differences depending on the job position, as well as whether the differences depending on the number of hours spent on the Internet per day or the completed cyber training are the same on average for women and men, etc. can be studied. If there is one argument characteristic, then it is a one-way ANOVA model (Tooding, 2014). The following items are the basis for making decisions:

1. If the significance value is >0.05, there is no significant difference.

2. If the significance value is <0.05, there is a significant difference.

Statistical significance indicates the probability that the result or effect that was discovered was obtained purely by chance. Statistical significance is expressed by a p-value that falls between 0 and 1 (because there is a probability). A small p-value (0.01) indicates that the probability of chance is small (in this case only 1%). Therefore, for a p-value of 0.01, one can be 99% confident that the result is not random. Usually, $p = 0.05$ is considered the limit of statistical significance of the results. However, $p > 0.05$ does not necessarily mean that the observed result is also substantively significant. Here is where formulas cannot be blindly trusted. The assessment of the importance of the obtained results from the point of view of the study must be given to the author of the study. Consequently, results with a p-value slightly higher than 0.05 should not be automatically discarded (McLeod, 2023).

If the significance value is smaller than 0.05, it means there is a significant difference, and a further test called a post-hoc test should be used to find out the difference (Candiwan et al., 2022, 233). It is used after performing a one-way ANOVA. ANOVA can say whether there are significant differences between the groups being studied, but it does not say which groups differ. Tukey's honestly significant difference test (Tukey HSD) is used to test the significance of differences in sample means. Tukey's HSD tests all pairwise differences while controlling for the probability of making one or more errors (Lane, 2012). A paired samples t-test is a hypothesis test for determining whether the population means of two dependent groups are the same. The test begins by selecting a sample of paired observations from the two groups. Thus, each observation in each group is paired (matched) with another observation from the other group. After that, the difference between each of these paired observations will be calculated and a one-sample t-test on these difference scores conducted (Stone, 2012)..

When there are only two characteristics to compare and ANOVA shows that there are significant differences between the scales, instead of the Tukey test, the Kruskal-Wallis test could be chosen, which shows more clearly where significant differences occur (Sonavala, 2024).

Invitations to participate were sent to the email addresses of 1,000 undergraduate students, 69 master's students, 439 faculty members and 271 staff members. A total of 277 employees and students from the Academy answered the questionnaire through LimeSurvey.

4. Results

4.1. General results

Table 1 describes how many people from each group were investigated. There were more women than men among the respondents. Among the age groups, most respondents were from the 41–50 age group (27%), followed by the 19–25 age group (30%) and 31–40 age group (19%). As much as 60% of respondents have completed cyber security training. Most people spend 1–5 hours a day on the Internet (52%), but there were also those who spent 11 or more hours a day on the Internet (3%). Outside of school, mobile Internet (48%) and private Wi-Fi networks (46%) are mainly used to access the Internet.

Table 1. Results of the respondents profile section (Kont, 2024, p. 93)

Characteristic	***Category***	***Number of respondents***	***Percentage***
Gender	Male	120	43%
	Female	157	57%
Age range	19–25	68	30%
	26–30	27	9%
	31–40	58	19%
	41–50	81	27%
	51–60	32	11%
	61-70	9	3%
	70+	2	1%
Position in the SKA	Vocational student	33	12%
	Under-graduate	98	35%
	Graduate	14	5%
	Lecturer	71	26%
	Administrative staff	42	15%
	Others	19	7%
Completed cyber security training	Yes	165	60%
	No	112	40%
Time range of Internet use	1-5 hours/day	145	52%
	6-10 hours/day	123	44%
	11 or more hours/day	9	3%
How do you access the Internet from outside your workplace?	Using Mobile Internet	133	48%
	Using public Wi-Fi network(Cafes, Shopping malls)	1	1%
	Using private Wi-Fi network (Home)	15	46%
	Using remote connection of my organization	128	5%

The question about their level of IT skills was not directly asked, because it is clear that basic computer literacy is required when studying, teaching, and working at a higher

education institution. In case of problems, an employee of the IT department is always there to help. The author of the study was more interested in the level of their cyber skills and whether or not they had completed the relevant training.

Table 2 shows the descriptive statistics obtained in the survey for all four defined categories – the Risky Behaviour Scale (RBS), Conservative Behaviour Scale (CBS), Exposure to Offence Scale (EOS) and the Risk Perception Scale (RPS). A score of 1 is considered the lowest and a score of 5 the highest value for each question.

Table 2. Descriptive statistics according to scales

Scale	No of questions	Average	Mean	Std. deviation	Std. error	Min	Max	Range
RBS	20	2,612	52,250	6,882	0,413	35	72	37
CBS	10	4,051	40,513	5,082	0,305	24	50	26
EOS	7	1,389	9,722	2,037	0,122	7	22	15
RPS	17	3,498	59,462	8,448	0,507	17	85	68

4.2. Research Question 1: Is there a significant difference between the surveyed groups (females and males) concerning their average score according to different behavioural scales (RBS, CBS, EOS, RPS)?

To answer the first research question, it is necessary to get an initial overview of the sample results and check whether the ANOVA assumption is met. For this purpose, the following are included: 1) descriptives – descriptive statistics about the results of the sample, 2) homogeneity of variance test – a test to check the equality of variances of the general set. Table 3 and Table 4 characterise the descriptive statistics and homogeneity of variances results according to the respondent's gender. According to Table 3, it can be seen that in the sample the average level (mean) of the comparable groups (men and women) is very similar according to the scales, while the dispersion of knowledge (standard deviation) is somewhat different. Can the resulting difference be generalised to the general population?

Table 3. Descriptive statistics of scales according to gender

	Gender	N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
RBS	Female	157	52,00	6,21	,50	35,00	67,00
	Male	120	52,58	7,69	,70	35,00	72,00
	Total	277	52,25	6,88	,41	35,00	72,00
CBS	Female	157	40,20	4,93	,39	24,00	50,00
	Male	120	40,93	5,27	,48	25,00	50,00
	Total	277	40,51	5,08	,31	24,00	50,00
EOS	Female	157	9,53	1,92	,15	7,00	16,00
	Male	120	9,98	2,16	,20	7,00	22,00
	Total	277	9,72	2,04	,12	7,00	22,00
RPS	Female	157	59,50	8,87	,71	24,00	85,00
	Male	120	59,42	7,90	,72	17,00	77,00
	Total	277	59,46	8,45	,51	17,00	85,00

Note: N (sample size), Mean (sample mean value), Std.Deviation (sample standard deviation)

Table 4. ANOVA tables according to gender

		Sum of Squares	df	Mean Square	F	Sig.
RBS	Between Groups	22,49	1	22,49	,47	,492
	Within Groups	13051,32	275	47,46		
	Total	13073,81	276			
CBS	Between Groups	36,00	1	36,00	1,40	,238
	Within Groups	7093,20	275	25,79		
	Total	7129,21	276			
EOS	Between Groups	13,55	1	13,55	3,29	,071
	Within Groups	1132,05	275	4,12		
	Total	1145,60	276			
RPS	Between Groups	,44	1	,44	,01	,938
	Within Groups	19698,42	275	71,63		
	Total	19698,85	276			

Sig. = significance probability p; Levene Statistic = a statistic that expresses the magnitude of the difference

According to Table 4, since $p > \alpha$ for all four scales, it is proven that $p > \alpha$ and H_0 remains valid. Therefore, it can be said with confidence that there are no significant differences between men and women across the scales.

4.3. Research Question 2: Is there a significant difference between the surveyed groups (students, academics and administrative staff) concerning their average score according to different behavioural scales (RBS, CBS, EOS, RPS)?

To answer the second research question and perform a comparative analysis with other similar studies, the data of the respondents' position was grouped into three groups (students, academics, administrative staff) and four scales instead of the six surveyed groups (i.e. vocational students, undergraduate students, graduate students, lecturers, administrative staff and others).

Table 5. Descriptive statistics of scales according to the position

	Position	N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
RBS	Student	146	53,60	6,95	,57	35,00	70,00
	Academic	89	49,81	6,75	,72	35,00	72,00
	Administrative	42	52,71	5,53	,85	40,00	64,00
	Total	277	52,25	6,88	,41	35,00	72,00
CBS	Student	146	38,81	5,22	,43	24,00	50,00
	Academic	89	42,83	4,27	,45	30,00	50,00
	Administrative	42	41,52	3,91	,60	31,00	47,00
	Total	277	40,51	5,08	,31	24,00	50,00
EOS	Student	146	9,77	2,14	,18	7,00	22,00
	Academic	89	9,47	1,88	,20	7,00	16,00
	Administrative	42	10,07	1,98	,31	7,00	16,00
	Total	277	9,72	2,04	,12	7,00	22,00
RPS	Student	146	59,50	8,67	,72	24,00	85,00
	Academic	89	58,90	9,00	,95	17,00	81,00
	Administrative	42	60,52	6,26	,97	46,00	75,00
	Total	277	59,46	8,45	,51	17,00	85,00

Table 5 presents the descriptive statistics of the various member groups of the Academy. The sample shows that the average level (mean) of the comparable groups (students, academics, administrative staff) is very different, especially in the RBS and CBS scales. Can the resulting difference be generalised to the general population?

Table 6. ANOVA tables according to the position

		Sum of Squares	df	Mean Square	F	Sig.
RBS	Between Groups	806,53	2	403,26	9,01	,000
	Within Groups	12267,28	274	44,77		
	Total	13073,81	276			
CBS	Between Groups	945,63	2	472,81	20,95	,000
	Within Groups	6183,58	274	22,57		
	Total	7129,21	276			
EOS	Between Groups	11,09	2	5,54	1,34	,264
	Within Groups	1134,51	274	4,14		
	Total	1145,60	276			
RPS	Between Groups	75,79	2	37,89	,53	,590
	Within Groups	19623,07	274	71,62		
	Total	19698,85	276			

As shown in Table 6, there are at least two groups representing populations with different levels (RBS and CBS). Post-hoc tests must then be used to see which groups' mean values are significantly different. The Tukey test compares group means pairwise. First, the RBS average means of the two groups are compared. In Table 6, the most important behaviour scales are RBS and CBS, the other two scales are given only for the sake of clarity.

1. RBS (students and academics)
Ho: μStudents = μAcademic
H_1: μStudents < μAcademic
α = 0.05
Conclusion: According to the probability of significance (0.000, e.g. 0%), H_1 has been proved. The mean scores of these groups considering the RBS are statistically significantly different.

2. RBS (students and administrative staff)
Ho: μStudents = μAdministrative
H_1: μStudents < μAdministrative
α = 0.05
Conclusion: According to the probability of significance (0.729, e.g. 72.9%), Ho remains true. The mean scores of these groups considering the RBS generally do not differ.

3. RBS (academics and administrative staff).
Ho: μAcademic = μAdministrative
H1: μAcademic < μAdministrative
α = 0.05
Conclusion: According to the probability of significance (0.090, e.g. 9%), Ho remains true. The mean scores of these groups considering the RBS of these groups generally do not differ.

Table 7. The Tukey test according to position

	Position		Mean Difference (I - J)	Std. Error	Sig.
Tukey HSD (RBS)	Student	Academic	3,79	,90	,000
		Administr.	,89	1,17	,729
	Academic	Student	-3,79	,90	,000
		Administr.	-2,91	1,25	,055
	Administrative	Student	-,89	1,17	,729
		Academic	2,91	1,25	,055
Tukey HSD (CBS)	Student	Academic	-4,02	,64	,000
		Administr.	-2,72	,83	,004
	Academic	Student	4,02	,64	,000
		Administr.	1,31	,89	,307
	Administrative	Student	2,72	,83	,004
		Academic	-1,31	,89	,307
Tukey HSD (EOS)	Student	Academic	,30	,27	,513
		Administr.	-,30	,36	,682
	Academic	Student	-,30	,27	,513
		Administr.	-,60	,38	,259
	Administrative	Student	,30	,36	,682
		Academic	,60	,38	,259
Tukey HSD (RPS)	Student	Academic	,60	1,14	,858
		Administr.	-1,02	1,48	,769
	Academic	Student	-,60	1,14	,858
		Administr.	-1,62	1,58	,561
	Administrative	Student	1,02	1,48	,769
		Academic	1,62	1,58	,561

Similar conclusions can be drawn for other behaviour scales. The mean scores of students and academics as well as students and administrative staff groups considering the CBS are statistically significantly different but between academics and administrative staff, the CBS of these groups generally does not differ. Thus, it can be concluded that the cause of the differences in the RBS and the CBS is the student group. These results coincide with the Öğütçü et al. (2016) study, which also revealed that it was the students who created a significant difference between the surveyed groups, while the Benavides-Astudillo et al. (2022) study determined that the academic group had significant differences with the administrative staff and student groups.

4.4. Does the duration of time spent on the Internet affect the average of the scales (RBS, CBS, EOS, RPS)?

To answer the third research question, respondents were grouped into three ranges according to how much time per day they use the Internet (i.e. 1 to 5 hours/day, 6 to 10 hours/day, and 11 or more hours/day). Table 8 presents descriptive statistics for various Internet users. It can be seen that there are no significant differences between the averages of the CBS and RPS scales, but for the EOS and RBS scales, the group that uses the Internet 11 or more hours/day clearly stands out in terms of the average indicator. The same difference can be noticed in the case of this group in the dispersion (standard deviation). Can the resulting difference be generalised to the general population?

Table 8. Descriptive statistics according to the Internet use time per day

Internet use per day		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
RBS	1-5 hours/day	145	51,09	6,68	,55	35,00	68,00
	6-10 hours/day		53,07	6,60	,60	38,00	69,00
	11+ hours/day	9	59,67	8,35	2,78	44,00	72,00
	Total	277	52,25	6,47	,41	35,00	72,00
CBS	1-5 hours/day	145	40,19	5,25	,44	24,00	50,00
	6-10 hours/day	123	40,88	4,92	,44	25,00	49,00
	11+ hours/day	9	40,67	4,74	1,58	35,00	46,00
	Total	277	40,51	5,08	,31	24,00	50,00
EOS	1-5 hours/day	145	9,77	2,09	,17	7,00	22,00
	6-10 hours/day	123	9,56	1,91	,17	7,00	16,00
	11+ hours/day	9	11,11	2,47	,82	7,00	14,00
	Total	277	9,72	2,04	,12	7,00	22,00
RPS	1-5 hours/day	145	59,08	8,81	,73	17,00	85,00
	6-10 hours/day	123	60,00	8,23	,74	24,00	79,00
	11+ hours/day	9	58,22	5,02	1,67	50,00	68,00
	Total	277	59,46	8,45	,51	17,00	85,00

Table 9 shows the ANOVA analysis, which shows that there is a significant difference between the other scales and the RBS scale with a value of $p = 0.000$. Therefore, there is a significant difference between the Internet usage times of the participants. This confirms that at least two groups have a statistically significant difference in their level of RPS.

Table 9. ANOVA tables according to the Internet use time per day

		Sum of Squares	df	Mean Square	F	Sig.
RBS	Between Groups	773,64	2	386,82	8,62	,000
	Within Groups	12300,18	274	44,89		
	Total	13073,81	276			
CBS	Between Groups	31,44	2	15,72	,61	,546
	Within Groups	7097,76	274	25,90		
	Total	7129,21	276			
EOS	Between Groups	20,92	2	10,46	2,55	,080
	Within Groups	1124,67	274	4,10		
	Total	1145,60	276			
RPS	Between Groups	70,29	2	35,14	,49	,613
	Within Groups	19628,56	274	71,64		
	Total	19698,85	276			

Note: SS = Sum of Squares; DF = Degree of Freedom; MSe = Mean of squares; F = Error; SIG = Significant at .05 level of significance

To find out in which group this difference occurs, the Tukey test was applied between groups Internet use time per day, to see which groups' mean values in RBS are significantly different if the group means are compared pairwise (see Table 13). First, the RBS average means of the two groups are compared.

1. RBS (1–5 hours/day and 6–10 hours/day).
Ho: μ1–5 hours/day = μ6–10 hours/day
H_1: μ1–5 hours/day < μ6–10 hours/day
$\alpha = 0.05$
Conclusion: According to the probability of significance (0.043, e.g. 4,3%), H_1 has been proved. The mean scores of these groups considering the RBS are statistically significantly different.

2. RBS (1–5 hours/day and 11 and more hours/day)
Ho: μ1–5 hours/day = μ11 and more hours/day
H_1: μ1–5 hours/day < μ11 and more hours/day
$\alpha = 0.05$
Conclusion: According to the probability of significance (0.001, e.g. 0.1%), H_1 has been proved. The mean scores of these groups considering the RBS are statistically significantly different.

3. RBS (6–10 hours/day and 11 and more hours/day)
Ho: μ6–10 hours/day = μ11 and more hours/day
H_1: μ6–10 hours/day < μ11 and more hours/day
$\alpha = 0.05$

Conclusion: According to the probability of significance (0.013, e.g. 1.3%), H_1 has been proved. The mean scores of these groups considering the RBS are statistically significantly different.

Table. 10. Results obtained in the Tukey test between the groups (1–5 hours/day, 6–10 hours/day and 11 or more hours/day) and the scale (RBS)

Position			Mean Difference (I - J)	Std. Error	Sig.
Tukey HSD (RBS)	1-5 hours/day	6 -10 hours/ day	-1,98	,82	,043
		11+ hours/ day	-8,58	2,30	,001
	6 -10 hours/ day	1-5 hours/day	1,98	,82	,043
		11+ hours/ day	-6,59	2,31	,013
	11+ hours/ day	1-5 hours/day	8,58	2,30	,001
		6 -10 hours/day	6,59	2,31	,013

Thus, it can be concluded that the cause of the differences in the RBS are the groups who spend 11 or more hours/day and 6–10 hours/day on the Internet. They are the weakest link. The results obtained by applying the post-hoc Tukey test on the RBS scale show that the respondents of the groups who spend 6–10 hours/day and 11 or more hours/day on the Internet are more tolerant of risky situations than the groups who spend less time on the Internet (see Table 9). In risky situations, they are more at risk than groups that spend less time on the Internet. These results coincide with Öğütçü et al. (2016) and Benavides-Astudillo et al. (2022) findings. In both studies, it was found that the significant difference occurs precisely on the RBS scale.

4.5. Does the cyber security training attendance or non-attendance affect the average of the scales (RBS, CBS, EOS, RPS)?

Finally, to answer the fourth research question, a test of whether participation in security training affects the mean scale scores was conducted. Respondents were surveyed in two groups, divided into those who had participated in cyber security training and those who had not.

Table 11 presents the descriptive statistics for those who answered that they have completed the training and for those who answered that they have not participated in the training. The smallest difference is the average level (mean) for the EOS scale, but there is a difference in the dispersion between those who have passed and those who have not, in every scale (standard deviation).

Table 11. Descriptive statistics according to the cyber security training

Passed Cyber Security Training		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
RBS	Yes	165	51,19	6,34	,49	35,00	72,00
	No	112	53,81	7,37	,70	35,00	70,00
Total		277	52,25	6,88	,41	35,00	72,00
CBS	Yes	165	42,00	4,71	,37	25,00	50,00
	No	112	38,32	4,83	,46	24,00	49,00
Total		277	40,51	5,08	,31	24,00	50,00
EOS	Yes	165	9,65	1,76	,14	7,00	16,00
	No	112	9,83	2,40	,23	7,00	22,00
Total		277	9,72	2,04	,12	7,00	22,00
RPS	Yes	165	61,58	7,32	,57	34,00	85,00
	No	112	56,34	9,04	,85	17,00	79,00
Total		277	59,46	8,45	,51	17,00	85,00

The fourth research question was also tested at a significance level of $\alpha = 0.05$. Table 11 shows the ANOVA analysis, which indicates that there is a significant difference between the EOS with a significance value of $p > 0.05$ and other scales with a value of $p = 0.000$. Therefore, there is a significant difference between the participants who have completed cyber security training and those who have not in their level of RBS, CBS and RPS.

Table 12. ANOVA tables according to the passed cyber security training

		Sum of Squares	df	Mean Square	F	Sig.
RBS	Between Groups	459,57	1	459,57	10,02	,002
	Within Groups	12614,24	275	45,87		
	Total	13073,81	276			
CBS	Between Groups	902,78	1	902,78	39,87	,000
	Within Groups	6226,43	275	22,64		
	Total	7129,21	276			
EOS	Between Groups	2,21	1	2,21	,53	,467
	Within Groups	1143,39	275	4,16		
	Total	1145,60	276			
RPS	Between Groups	1833,60	1	1833,60	28,22	,000
	Within Groups	17865,25	275	64,96		
	Total	19698,85	276			

Since there are only two comparable characteristics, it was decided to use the MPAR (nonparametric) Kruskal-Wallis test instead of Tukey's test. It shows more clearly in which scales the largest and smallest mean differences occur between respondents who had undergone cyber security training and those who had not. According to Table 13, the mean rank of the respondents who passed cyber security training and who have not passed this training, has large differences in the CBS, 163.09 for respondents who have completed the training and 103.50 for respondents who have not. The other significant difference is in the RPS, where respondents who passed cyber security training scored 158.83 as a mean rank, and non-passed respondents gained 109.78 as a mean rank. However, these two scales are united by the fact that the average of respondents who have undergone cyber training is significantly higher than the average of those who have not completed the training. On the other hand, the results are opposite in the case of the RBS scale – those who passed the cyber security training gained 126.37 as a mean rank while those who have not completed the training gained 157.60 as a mean rank. Exposure Offence is not at all affected by completed cyber security training.

Table 13. Ranks according to the completion of cyber security training

		N	Mean Rank
RBS	Yes	165	126,37
	No	112	157,60
	Total	277	
CBS	Yes	165	163,09
	No	112	103,50
	Total	277	
EOS	Yes	165	139,08
	No	112	138,89
	Total	277	
RPS	Yes	165	158,83
	No	112	109,78
	Total	277	

According to the probability of ANOVA significance (Sig. = 0.467, e.g. 46.7%), Ho remains true for EOS. The mean rank of those who have completed cyber security training considering the Exposure Offence of these groups generally do not differ. This can be explained by the fact that the people working and studying at the Academy are certainly more careful about cyber offences than average – future specialists are prepared here for rescue, finance, justice, and police and border guard.

Finally, a selection of the respondents' own opinions about the survey and the topics covered in the questionnaire is presented:

- *In principle, everything can be dangerous, but some environments need to be used. It would be safest to live offline.*

- *My internet usage outside of work: mobile data and home wifi. As far as I know, different communication environments have different levels of security. I never share sensitive information on FB Messenger, but I have done so on Signal. Online shopping and entering data - if I do it in the safest places I know, I don't consider it a problem, but I would never go shopping in a less-known Estonian store or in a foreign online environment.*
- *If you understand where to press and what to share, there are no problems. The more you participate in Facebook sharing games, the more problems you have.*
- *Everything depends on the nature of the activity, the information used, previous awareness, etc.*
- *A common peasant mind must be maintained in the Internet environment as well as in a normal environment.*
- *Several of the aforementioned activities can be dangerous, but it is necessary to consider the justification and check the existence of security solutions (e.g. in the case of Internet banking), whether there is secure authentication and the correct website, before opening emails with advertising content, the authenticity of the sender and to be sure that there is any interest in such emails against letters, etc. On the other hand, the use of public Wi-Fi should be avoided in any case and rather use mobile data communication, which is now quite affordable, than looking for it from various service providers in Estonia. Checking the identity card number by security personnel when entering the building – again, the possibility of benefit and harm should be assessed – e.g. if the fire escape is secured by a contract security company, then it may be absolutely necessary, but it should be avoided in the case of arbitrary fire escapes. In the case of file sharing and chat programs and AI, it is simply necessary to avoid entering sensitive texts, in which case the benefits of sharing information outweigh the possible dangers.*
- *Even paid movies/music/software, etc. may contain malware. In addition, opening the email itself should not be dangerous, opening and saving or viewing a file/link, etc. attachment contained in the email is.*
- *In my opinion, all actions on the Internet are already very dangerous – and at the same time, you cannot stop using the Internet. Everything already goes through the Internet or services, etc. always need a permanent connection.*

5. Conclusions

In this study, students, lecturers (researchers) and employees of the Academy were investigated in terms of hybrid threats and cyber security-related risk prevention options such as risky behaviour, conservative behaviour, exposure to offence and risk perception. The present study is part of a larger study conducted within the framework of the hybrid threat cooperation programme (HYBRIDC).

Four research questions were raised and all of them were answered during the analysis of the results. Previous research highlights the role of gender in shaping cybersecurity attitudes and behaviours shows that males tend to have better awareness of online safety. In current study it can be seen that there is no significant difference in the cyber behaviour scales of women and men in the RBS, CBS score and RPS score types, although it must

be emphasized that the mean of men (mean severe) is slightly higher than that of women. However, there is a significant difference in the EOS scale. According to the results, the more the respondents perceive threats, the more defensive their behaviour becomes. Therefore, based on the results, it can be said that men's exposure to danger has been higher and they are accordingly more careful.

Research shows that while students often have awareness of cyber threats, this is not always reflected in safe behavior. The current study suggests that there are no significant differences in EOS and RPS score types among faculty, administrative staff and students. However, it can be seen that the proportion of students using risky information technologies is higher than in other groups. For example, students' exposure to threat scale scores are higher than other groups. Conservative behaviour is also not as well developed for students as it is for academics and administrative staff. All this shows that students are more vulnerable to risks.

To explore the relationship between daily internet usage and cybersecurity behaviours, respondents were grouped into three categories based on usage time: 1–5 hours, 6–10 hours, and 11 or more hours per day. The EOS and RBS scales showed noticeable differences, particularly among those using the internet for 11 or more hours daily, who scored higher and showed greater variability. ANOVA analysis confirmed a statistically significant difference in the RBS scale across groups, indicating that internet usage time influences risky online behaviour. The reseults showed that the most significant differences occur between those using the internet 6–10 hours and 11+ hours per day - they are more tolerant of risky behaviour compared to those with lower usage. We can cinclude that as the use of technology increases during the day, people are exposed to more risks, but at the same time, their perception of danger and conservative behaviour increase.

Trained and knowledgeable employees reduce the likelihood of accidental and unintentional actions that could lead to violations of cyber security policies, and play a key role in minimizing information security risks and safeguarding the organization's critical assets and sensitive personal data. Only 60% of respondents have completed cyber security training, which is obviously too few considering that the Academy is the most important school in Estonia in the field of internal security. This fact in itself shows that more training needs to be done. While there is no significant difference between the EOS scores of the group that received security training and the group that did not receive such training, the CBS score and RPS score of the first group are significantly higher than the score of the second group. This result clearly shows that such training increases people's awareness.

The open answers of the respondents expressed a range of cautious and pragmatic views about internet use and digital security. Many believe that while everything online can potentially be dangerous, risk can be managed by being informed and selective about platforms and activities. They stressed the importance of common sense, secure environments, and avoiding untrusted sources—particularly when shopping or using public Wi-Fi. Several noted that secure authentication and awareness of sender authenticity are key when handling emails. Others highlighted the risks of sharing sensitive data via chat apps or participating in social media games. Despite widespread concerns, respondents acknowledged that avoiding the internet altogether is unrealistic given its necessity in modern life.

Future studies could build upon this recent study by expanding the sample size and replicating the research across diverse organizational and educational settings. This would enhance the generalizability of the findings and help validate the applicability of the research model in different contexts. Moreover, incorporating new respondent groups would allow for a broader understanding of cybersecurity behaviours across various demographics. Such replication efforts could yield valuable insights for the development of targeted information security training programmes and policies, enabling organizations to implement more effective, context-specific cybersecurity measures.

References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. DOI: 10.1016/j.chb.2016.12.040.

Bederna, Z., Szadeczky, T. (2020). Cyber espionage through Botnets. *Security Journal*, 33, 43–62, DOI: 10.1057/s41284-019-00194-6.

Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Rámos, R., Fuertes, W., Fernández-Peña, F., Sanchez-Gordon, S., Bastidas-Chalan, R. (2022). Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior, in: *International Conference on Applied Technologies, Springer International Publishing*, Cham, pp. 351-364, DOI: 10.1007/978-3-031-03884-6 26.

Busvine, D., Kaeckenhoff, T. (2020). Prosecutors open homicide case after hacker attack on German hospital, *Reuters*, September 18, https://www.reuters.com/article/us-germany-cyber-idUSKBN26926X

Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. *International Journal of Safety and Security Engineering*, 12(2), 229-237. DOI: 10.18280/ijsse.120212.

Ceran, O., Karataş, S. (2021). Individual differences on conservative and risky behaviors about information security. *Bilişim Teknolojileri Dergisi*, 14(2), 161-170, https://dergipark.org.tr/en/download/article-file/990584

Concepcion, J. D., Palaoag, T. D. (2024). An Assessment of Cybersecurity Awareness among Academic Employees at Quirino State University: Promoting Cyber Hygiene. *Journal of Electrical Systems*, 20(7s), 769-775. 390. DOI: 10.52783/jes.3445.

Duman, F. K. (2022). Determining Cyber Security-Related Behaviors of Internet Users: Example of the Faculty of Sport Sciences Students. *European Journal of Education*, 5(1), 112-128. DOI: 10.26417/723gru15.

Einmann, A. (2020). Iranian intelligence attempted to access University of Tartu email accounts (Estonian). *Postimees*, April 14, https://www.postimees.ee/6949265/iraani-luure-uritas-ligipaasu-tartu-ulikooli-e-posti-kontodele.

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In Psychological and behavioral examinations in cyber security (pp. 46-63). IGI Global. DOI: 10.4018/978-1-5225-4053-3.ch003.

Hirsjärvi, S., Remes, P., Sajavaara, P. (2020). *Research and Write* (Estonian). Medicina, Tartu, 2010.

Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*, John Wiley & Sons.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, 51(1), 69–79. DOI: 10.1016/j.im.2013.10.001.

Iiskola, J. (2019). *Measuring Cybersecurity* (Finnish), Haaga-Helio Amattikorkeakoulu OY. https://urn.fi/URN:NBN:fi:amk-201905159951

Jalali, M.S., Bruckes, M., Westmattelmann, D., Schewe, G. (2020). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*, 22(1):e16775. DOI: 10.2196/16775.

Jeske, D., van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, 66, 129-41. DOI: 10.1016/j.cose.2017.01.010.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, Penttinen, A., Porvari, P., Talala, T. (2014). *Corporate Risk Management* (Finnish). Finanssi- ja vakuutuskustannus Oy.

Kansallinen riskiarvio, Sisäinen turvallisuus (Finnish). (2024). *Sisäministeriön julkaisuja*, 4, 2023. http://urn.fi/URN:ISBN:978-952-324-602-7.

Karu, L. (2020). The cyber attack that hit the health care college disrupted the servers (Estonian). *Tartu Postimees*, September 15, https://tartu.postimees.ee/7062330/tervishoiukorgkooli-tabanud-kuberrunnak-loi-serverid-sassi.

Kont, K.-R. (2024). Cybersecurity behaviours of the employees and students at the Estonian Academy of Security Sciences. *Organizational Cybersecurity Journal: Practice, Process and People*, 4(2), 85-104. https://doi.org/10.1108/OCJ-02-2024-0001.

Kont, K.-R. (2023). Presentation at the Eighth International Conference on Cyber-Technologies and Cyber-Systems. https://www.iaria.org/conferences2023/filesCYBER23/CYBER_80056.pdf

Kuusela, H., Ollikainen, R. (2005). Risks and Risk Management Thinking, (Finnish) in: Risks and Risk Management, Tampere University Press, Tampere. https://trepo.tuni.fi/bitstream/handle/10024/65418/riskit_ja_riskienhallinta_2005.pdf?sequence=1

Lane, D. M. (2012). *Tukey's Honestly Significant Difference (HSD)*, in: Neil J. Salkind, Encyclopedia of Research Design. DOI: 10.4135/9781412961288.

Limnéll, J., Majewski, K., Salminen, M. (2014). *Cybersecurity*, Docendo.

McLeod, S. (2023). P-Value And Statistical Significance: What It Is & Why It Matters. *Simply Psychology*. https://www.simplypsychology.org/p-value.html.

Mian, T. S., Alatawi, E. M. (2023). Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector, Humanities & Natural Sciences Journal 4(9), 101–114. DOI: 10.53796/hnsj498.

Noran, S. F. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6(2). 137-154, DOI: 10.1080/23738871.2021.1973526

Ög˜ütçü, G., Testik, Ö. M., Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93. DOI: 10.1016/j.cose.2015.10.002.

Oxford Dictionary (2019). https://en.oxforddictionaries.com/definition/cyberthreat

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 24(2), 371-390.

Qashqari, A., Munshi, A., Alturkstani, H., Ghwati, H., Alhebshi, D. (2020). *The Human Factors and Cybersecurity Policy* [Ebook]. Hämtad från http://paper.ijcsns.org/07_book/202004/20200401.pdf

Roman, J. (2015). Universities: prime breach targets. https://www.databreachtoday.asia/universities-prime-breach-targets-a-7865

Seppänen, T. (2022). Changing security environment and information security in higher education institutions (Finnish) . *Current information security review*, 12. https://blogs.helsinki.fi/thinkopen/tietoturvakatsaus-2022-12/

Shad, M. R. (2019). Cyber threat landscape and readiness challenge of Pakistan. *Strategic Studies*, 39 (1), 1–19, DOI: 10.53532/ss.039.01.00115.

Sonawala, J. (2024). Exploring Statistical Analysis with the Kruskal-Wallis Test. https://www.linkedin.com/pulse/exploring-statistical-analysis-kruskal-wallis-test-jvalin-sonawala-i4occ/.

Stone, E. R. (2012). *t Test, Paired Samples*. In: Neil J. Salkind, Encyclopedia of Research Design, 2012, DOI: 10.4135/9781412961288.

Svitek, P., Anderson, N. (2014). University of Maryland computer security breach exposes 300,000 records, *The Washington Post*, February 19, https://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/19/ce438108-99bd-11e3-80ac63a8ba7f7942_story.html.

Tooding, L-M. (2014). *Social analysis methods and methodology training database* (Estonian). *Analysis of Variance*, 2014, https://samm.ut.ee/dispersioonanalyys.

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. International *Journal of STEM Education for Sustainability*, 3(1), 47-67. DOI: 10.52889/ijses.v3i1.132.

Verkijika, S. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers In Human Behavior*, 101, 286-296. DOI: 10.1016/j.chb.2019.07.034.

Widup, S., Maxwell, K., Baker, W., Porter, C., Jacobs, J., Thompson, K., Spitler, M., Hylender, D., Brannon, S., Gilbert, K. (2013). 2013 verizon data breach investigations report, Technical report, Verizon. DOI: 10.13140/RG.2.1.4729.8647.

Widup, S., Spitler, M., Hylender, D., Bassett, G. (2018). 2018 verizon data breach investigations report, Technical report, Verizon. https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigayions_Report.

Yerby, J., Floyd, K. (2018). Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information Systems Security Education*, 6(1). 23-23, https://cisse.info/journal/index.php/cisse/article/view/90/CISSE_v06_i01_p05.pdf

Yiğit, M. F., Seferoğlu, S. S. (2019). Investigating students' cyber security behavior in relation to big five personality traits and other various variables. *Mersin University Journal of the Faculty of Education*, 15(1), 186–215. DOI: 10.17860/mersinefd.437610.

Zimmermann, V., Renaud, K. (2021). The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions, *ACM Transactions on Computer-Human Interaction* 28(1), 1–45. DOI: 10.1145/3429888.

Received February 22, 2025, revised May 3, 2025, accepted June 15, 2025