TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Luka Kerin 233934IVCM

CYBERSECURITY KNOWLEDGE AND BEHAVIOUR AMONG SLOVENIANS

Master's Thesis

Supervisor: Ricardo Gregorio Lugo
PhD.

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Luka Kerin 233934IVCM

SLOVEENIDE KÜBERTURVALISUSE ALASED TEADMISED JA KÄITUMINE

Magistritöö

Juhendaja: Ricardo Gregorio Lugo
PhD.

Tallinn 2025

Author's Declaration of Originality

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

Author: Luka Kerin

18.05.2025

Abstract

The increasing frequency and severity of cyber incidents in Slovenia highlights a pressing need to understand how individuals perceive and practise cybersecurity. This study investigates the current state of cybersecurity knowledge, behaviour, and self-efficacy among Slovenians, aiming to identify gaps between perceived competence and actual security practices. A mixed-methods approach was employed, combining validated instruments such as the Self-Efficacy for Information Security (SEIS) scale and cognitive-behavioural assessments with statistical analysis performed using JASP. Data were gathered from a diverse cross-section of the population via a structured online survey. The results reveal significant demographic disparities in self-efficacy, knowledge, and behaviour, particularly along lines of gender, education, and perceived expertise. A consistent gap was identified between what respondents believed about their cybersecurity competence and their actual practices, echoing the well-documented privacy paradox. Furthermore, regression and mediation analyses confirmed that knowledge partially mediates the relationship between self-efficacy and behaviour. These findings underscore the limitations of awareness campaigns and the importance of tailored educational interventions. The study contributes novel, population-specific insights into the Slovenian context and proposes evidence-based recommendations for national cybersecurity policy, educational curricula, and future research directions.

The thesis is written in English and is 78 pages long, including 6 chapters, 5 figures and 57 tables.

Annotatsioon

Sloveenide küberturvalisuse alased teadmised ja käitumine

Sloveenias sagenenud ja tõsisemaks muutunud küberintsidendid osutavad tungivale vajadusele mõista, kuidas inimesed küberohte tajuvad ja milliseid turbekäitumisi nad tegelikult rakendavad. Käesolev uurimistöö käsitleb sloveenlaste teadmisi, käitumist ja enesetõhusust küberjulgeoleku valdkonnas, eesmärgiga tuvastada vastuolusid tajutud pädevuse ja tegelike praktikate vahel. Uuringus kasutati kombineeritud metoodikat, milles ühendati valideeritud instrumendid, nagu teabekaitse enesetõhususe skaala (SEIS), ning kognitiiv-käitumuslikud hinnangud koos statistilise analüüsiga JASP-i keskkonnas. Andmed koguti mitmekesise elanikkonna seas veebipõhise küsimustiku abil. Tulemused näitasid märkimisväärseid demograafilisi erinevusi enesetõhususe, teadmiste ja käitumise osas, eriti soo, haridustaseme ja tajutud ekspertsuse lõikes. Korduvalt ilmnes lõhe vastanute subjektiivsete hinnangute ja tegeliku turbekäitumise vahel, peegeldades niinimetatud privaatsusparadoksi. Regressiooni- ja mediatsioonianalüüs kinnitasid, et teadmised vahendavad osaliselt seost enesetõhususe ja käitumise vahel. Uurimistulemused toovad esile teavituskampaaniate piirangud ja kohandatud hariduslike sekkumiste olulisuse. Käesolev magistritöö pakub uudseid, kontekstitundlikke teadmisi Sloveenia kohta ning esitab tõenduspõhiseid soovitusi riikliku küberjulgeolekupoliitika, haridusprogrammide ja edasiste uuringute tarbeks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 78 leheküljel, 6 peatükki, 5 joonist, 57 tabelit.

List of Abbreviations and Terms

ANOVA	Analysis of Variance
BCISQ	Cognitive Internet Security Questionnaire
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CS	Computer Science
EU	European Union
GDPR	General Data Protection Regulation
GEI	General Controllability
HSD	Honestly Significant Difference
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IS	Information Security
IT	Information Technology
MANOVA	Multivariate Analysis of Variance
MFA	Multi-Factor Authentication
MRQ	Main Research Question
NSA	National Security Agency
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SEIS	Self-Efficacy for Information Security
SRQ	Sub-research Question
URSIV	Slovenian Government Information Security Office
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Table of Contents

1 Introduction 10

1.1 Motivation and Research Problem 10

1.2 Research questions 12

1.3 Scope and Limitation 13

2 Literature Review 15

2.1 Literature Review Method 15

2.2 Review of Existing Research 16

2.3 Definition of Key Terms 26

2.4 Research Questions: Preliminary Findings from Literature 27

3 Research Methodology 30

3.1 Subjects 30

3.2 Instruments 30

3.3 Procedure 32

4 Data Analysis and Results 33

4.1 Overview of the Chapter 33

4.2 Demographic Distribution of Respondents 33

4.3 Data Normality 35

4.4 Correlation Analysis 35

4.5 Gender Differences in Self-Efficacy, Controllability, Knowledge, and Behaviour 36

4.6 Educational Differences 37

4.6.1 Educational Differences in SEIS 37

4.6.2 Educational Differences in GEI 39

4.6.3 Educational Differences in Cybersecurity Knowledge Scores . . . 40

4.6.4 Educational Differences in Cybersecurity Behaviour 42

4.7 Predicting Cybersecurity Behaviour from Knowledge, SEIS, and GEI . . 43

4.8 Mediation Analysis: The Role of Knowledge in the Relationship Between SEIS, GEI, and Behaviour 45

4.9 Predicting Cybersecurity Knowledge from SEIS and GEI 47

4.10 Differences in Cybersecurity Knowledge and Behaviour by Perceived Expertise 48

4.10.1 Differences in Cybersecurity Knowledge by Perceived Expertise . 48

4.10.2 Differences in Cybersecurity Behaviour by Perceived Expertise . . 50
4.11 Multivariate Differences in Knowledge and Behaviour by Perceived Expertise 52
4.12 Linear Regression: Predicting Cybersecurity Behaviour with Knowledge, SEIS, and GEI (Factoring Education, Gender, and Perceived Expertise) . . 53
4.12.1 Factoring Education 53
4.12.2 Factoring Gender 54
4.12.3 Factoring Perceived Expertise 55

5 Discussion and Interpretation 58
5.1 Chapter Overview 58
5.2 Discussion and Interpretation of Findings 58
5.3 Answering Research Questions 60
5.4 Study Limitations 62

6 Conclusions and Recommendations 64
6.1 Conclusions 64
6.2 Actionable Recommendations 65
6.3 Future Work 66

References 68

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis 75

Appendix 2 – SEIS and GEI Questions 76

List of Figures

1 *PRISMA literature review process* 15

2 *Predicting Cybersecurity Behaviour from Knowledge, Self-Efficacy, and General Controllability* 44

3 *Mediation Analysis: The Role of Knowledge in the Relationship Between SEIS, GEI, and Behaviour* 47

4 *Perceived Expertise and Knowledge Bar Plot* 49

5 *Perceived Expertise and Behaviour Bar Plot* 51

List of Tables

1 Descriptive statistics for categorical demographic variables 33
2 Gender Frequency Table 34
3 Education Frequency Table 34
4 Frequencies for Perceived expertise 34
5 Shapiro-Wilk Test 35
6 Spearman's Correlations 36
7 Independent Samples T-Test - Gender 37
8 Group Descriptives - Gender 37
9 ANOVA - Education and SEIS 37
10 Descriptives - Education and SEIS 38
11 Kruskal-Wallis Test - Education and SEIS 38
12 Standard HSD Post Hoc Comparisons - Education and SEIS 38
13 Dunnett Post Hoc Comparisons - Education and SEIS 38
14 ANOVA - Education and GEI 39
15 Descriptives - Education and GEI 39
16 Kruskal-Wallis Test - Education and GEI 39
17 Standard HSD Post Hoc Comparisons - Education and GEI 40
18 Dunnett Post Hoc Comparisons - Education and GEI 40
19 ANOVA - Education and Knowledge 40
20 Descriptives - Education and Knowledge 41
21 Kruskal-Wallis Test - Education and Knowledge 41
22 Standard HSD Post Hoc Comparisons - Education and Knowledge 41
23 Dunnett Post Hoc Comparisons - Education and Knowledge 41
24 ANOVA - Education and Behaviour 42
25 Descriptives - Education and Behaviour 42
26 Kruskal-Wallis Test - Education and Behaviour 42
27 Standard HSD Post Hoc Comparisons - Education and Behaviour 43
28 Dunnett Post Hoc Comparisons - Education and Behaviour 43
29 Model Summary - Predicting Behaviour 44
30 ANOVA - Predicting Behaviour 44
31 Coefficients - Predicting Behaviour 44
32 Direct effects 45
33 Indirect effects 45
34 Total effects 46
35 Path coefficients 46

36 R-Squared 46
37 Model Summary - SEIS, GEI and Knowledge 47
38 ANOVA - SEIS, GEI and Knowledge 47
39 Coefficients - SEIS, GEI and Knowledge 48
40 ANOVA - Perceived Expertise and Knowledge 48
41 Descriptives - Perceived Expertise and Knowledge 49
42 Post Hoc Comparisons - Perceived expertise 50
43 ANOVA - Perceived Expertise and Behaviour 50
44 Descriptives - Perceived Expertise and Behaviour 50
45 Post Hoc Comparisons - Perceived Expertise and Behaviour 51
46 MANOVA: Pillai Test 52
47 ANOVA: Perceived expertise - knowledge and behaviour 52
48 ANOVA: Perceived expertise - knowledge and behaviour 53
49 Model Summary: Factoring Education 53
50 ANOVA: Factoring Education 54
51 Coefficients: Factoring Education 54
52 Model Summary: Factoring Gender 55
53 ANOVA: Factoring Gender 55
54 Coefficients: Factoring Gender 55
55 Model Summary: Factoring Perceived Expertise 56
56 ANOVA: Factoring Perceived Expertise 56
57 Coefficients: Factoring Perceived Expertise 56

1. Introduction

1.1 Motivation and Research Problem

In today's connected digital world, individuals face a wide range of cybersecurity threats. While organisations typically have dedicated resources to address such risks, individuals are left on their own to secure themselves with what they know and buy. This difference in protection and preparedness makes personal cybersecurity a pressing issue.

To better understand and improve personal cybersecurity, it is necessary to examine the awareness, knowledge, and behaviour, which are key dimensions.

- **Awareness** refers to individuals' recognition of cybersecurity threats and the potential consequences of unsafe online behaviour [1].
- **Knowledge** encompasses an understanding of security concepts, such as password hygiene, safe browsing, and recognising social engineering tactics [2].
- **Behaviour** entails to the actual practices individuals adopt, like using strong passwords, enabling multi-factor authentication, and applying software updates.

However, evidence suggests that there is often a gap between awareness and behaviour. Individuals may be aware of risks but fail to adopt best practices due to low self-efficacy, underestimating the threat, or lack of motivation [3]. In Slovenia, the current state of individual cybersecurity is under-researched, though national reports indicate an increase in personal cyber incidents [4]. According to SI-CERT, they recorded 4587 incidents in 2024, which is roughly 1.7 times more than just 4 years before in 2020. These incidents are causing significant financial damage. Also according to SI-CERT's yearly report, the highest cost of an incident in 2024 was a 369,500 € crypto-investment scam, the average online shopping damage was 1,300 €, average damage in the case of interference in business communication was 33,000 €, and the highest attempted damage in mobile banking was 200,000 €.
Despite Slovenia's formal commitment to improve cybersecurity through its **Cyber Security Strategy**, the document lacks operational depth and fails to address the behavioural aspects of individual security. While it acknowledges the country's weaknesses and threats in this department, its strategy is vague, lacks concrete data, and offers no concrete solution [5]. The absence of concrete data on public awareness or behaviour further illustrates the reactive nature of the strategy. This gap underscores the need for research that not

only evaluates what Slovenians know and do regarding cybersecurity but also informs actionable recommendations.
On a government's website on national security, they also recognise cybersecurity to be an important part of it. They state that *the Cybersecurity Strategy thus determines measures for setting up a comprehensive national system to provide a high level of information security* [6]. However, as further discussed in Chapter 2, this document is far from *comprehensive*.

Slovenia's cybersecurity framework, as outlined by the NATO Cooperative Cyber Defence Centre of Excellence, reveals institutional ambition and structural fragmentation [7]. The governance is split across several key bodies: strategic coordination is managed by the Information Security Administration (ISA) under the Ministry of Public Administration, while operational incident response is handled primarily by SI-CERT, the national Computer Emergency Response Team. Military cyber capabilities fall under the Slovenian Armed Forces, particularly the Communication and Information Systems units. While this layered approach suggests a comprehensive national posture, the CCDCOE report identifies gaps in central coordination and legislative clarity [7]. Slovenia has no single authority with overarching jurisdiction for cybersecurity, which risks slowing response times and questionable accountability in cross-sector incidents. Moreover, the report highlights limited cyber threat intelligence sharing between civilian and military domains, raising concerns about interoperability in crisis scenarios. The national cybersecurity strategy remains under-implemented in practice, partly due to insufficient resourcing and the absence of enforcement mechanisms [7]. While Slovenia has laid the groundwork for a capable cybersecurity architecture, the realisation of its goals depends on overcoming bureaucracy and establishing clearer operational authority across sectors.

ENISA, the European Union Agency for Cybersecurity, emphasises that **individual cybersecurity competence** is a foundational element of national resilience [8]. Their guidelines call for member states to:

- Promote cybersecurity **education** across all age groups.
- Develop **policy frameworks** that support individual-level security measures.
- Launch **awareness campaigns** tailored to local cultural contexts [8].

The problem this thesis addresses is the **disconnect between individuals' perceived cybersecurity competence and their actual security practices**. In Slovenia, limited data exist on how citizens perceive, understand, and act upon cybersecurity threats (existing research is reviewed in chapter 2). This data could help policymakers and educators to design interventions that are both effective and culturally appropriate.

By critically examining the state of **cybersecurity knowledge, behaviour, and self-efficacy** among Slovenians, this study aims to generate practical insights that will:

- **Inform policy**: Expose the current cybersecurity state of diverse Slovenian demographic groups, which can be used to build evidence-based future strategies and policies.
- **Guide education**: Suggesting curriculum enhancements to boost cybersecurity literacy at multiple educational levels.
- **Support public campaigns**: Helping design culturally aligned awareness initiatives to encourage safe online practices.

Slovenia can benefit from a more resilient, informed public that can better protect itself in the cyber domain. This will help in reducing the national risk surface and contributing to broader European cybersecurity objectives, as outlined by ENISA's strategic priorities for member states [8]. Moreover, improving personal cybersecurity is essential for advancing Slovenia's digital transformation agenda, which aims to promote secure and widespread adoption of digital services in line with the European Commission's Digital Decade goals [9].

1.2 Research questions

1. **Main research question:** What is the current state of cybersecurity knowledge and behaviour among Slovenians?
   This question examines both knowledge and actual security practices among Slovenians, identifying potential gaps between awareness and behaviour.
2. **Sub-research question 1:** What is the level of self-efficacy for information security among Slovenians?
   This question will be answered using the SEIS (Self-Efficacy for Information Security) questionnaire to assess how confident individuals feel about their ability to protect their personal information and devices.
3. **Sub-research question 2:** What is the level of cybersecurity knowledge among Slovenians?
   This sub-question examines how well Slovenians understand key cybersecurity concepts, threats, and protective measures, such as password security, phishing, and multi-factor authentication.
4. **Sub-research question 3:** What are the actual cybersecurity behaviours of Slovenians?
   This investigates whether Slovenians follow best cybersecurity practices in daily life, including password management, software updates, safe browsing, and response to

security threats.

1.3 Scope and Limitation

This research focuses on personal cybersecurity practices among individuals in Slovenia, specifically examining the knowledge, behaviour, and self-efficacy in managing cybersecurity threats. The study aims to reveal how Slovenians perceive their own cybersecurity competence and how this perception aligns with their actual practices. By including psychological and behavioural dimensions, it offers a comprehensive, culturally informed analysis of personal cybersecurity within a national context.

The scope of this research is geographically confined to Slovenia and methodologically structured around self-reported survey data collected from a diverse population. While the findings are primarily intended to inform local policy, education, and awareness efforts, they may also contribute to broader academic discourse by demonstrating the necessity of context-specific cybersecurity strategies over generic, global approaches.

However, several limitations must be acknowledged to contextualise the findings and guide future work. First, the study's geographic and cultural specificity might limit the generalisability of its conclusions to other countries. While this local focus allows for a deeper understanding of Slovenian cybersecurity behaviours, it also reflects ENISA's recommendation for tailored national strategies that address unique societal contexts [8].

Second, the reliance on self-reported data introduces potential biases, including social desirability bias and inaccuracies in participants' self-assessment. Individuals may overestimate their cybersecurity abilities or underreport risky behaviours, a challenge commonly documented in behavioural cybersecurity research [10]. This limitation is particularly relevant when assessing self-efficacy, as the subjective nature of confidence may not always reflect actual competence [11].

Third, while the research aims for demographic diversity, achieving perfect representativeness is constrained by factors such as variations in willingness to participate and challenge to effectively reach the underrepresented groups. These factors could skew the dataset and require adjustments when doing the data analysis.

Fourth, the rapidly evolving nature of cyber threats poses a temporal limitation. As new technologies and attack vectors emerge, some findings may lose relevance over time. This reflects a broader issue in cybersecurity research, where insights can quickly become outdated [12].

Finally, the study provides a cross-sectional insight, displaying individual behaviours and knowledge at a single point in time. It does not assess how these factors might evolve in response to influences like policy changes, educational campaigns, or new threat landscapes. A longitudinal approach would be necessary to evaluate potential behavioural change and the long-term effectiveness of interventions.

These constraints highlight directions for future research, including the need for longitudinal studies and cross-country comparisons to enrich the field further.

2. Literature Review

2.1 Literature Review Method

To ensure that the literature review was conducted systematically and rigorously, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework was applied. PRISMA provides a structured approach for identifying, screening, and critically appraising sources, which helps to ensure transparency and comprehensiveness in the review process [13]. By following PRISMA guidelines, the literature review provides not only a simple summary of existing studies, but also offers a coherent, methodologically sound foundation that supports the credibility and academic integrity of this research.

More specifically, this literature review adopts a semi-systematic approach. It applies systematic principles to identify, screen, and synthesise relevant literature with critical rigour. The inclusion criteria required that studies address cybersecurity knowledge, behaviour, awareness, or self-efficacy, with preference given to empirical research and sources relevant to the Slovenian or European context. Exclusion criteria eliminated studies that focused purely on technical solutions without human-centred components or lacked sufficient methodological transparency; these criteria were applied during the abstract and full-text screening stages. The review included an initial total of 954 records, retrieved from academic databases including ACM Digital Library, IEEE Xplore, SpringerLink, and Scopus, with additional sources identified elsewhere. After the screening process, 24 records remained. An additional 8 records were manually identified from other sources. The result was 32 total references that were included in the literature review. These sources were selected based on relevance to cybersecurity knowledge, behaviour, self-efficacy, and national context or provided overall valuable insight for this thesis.

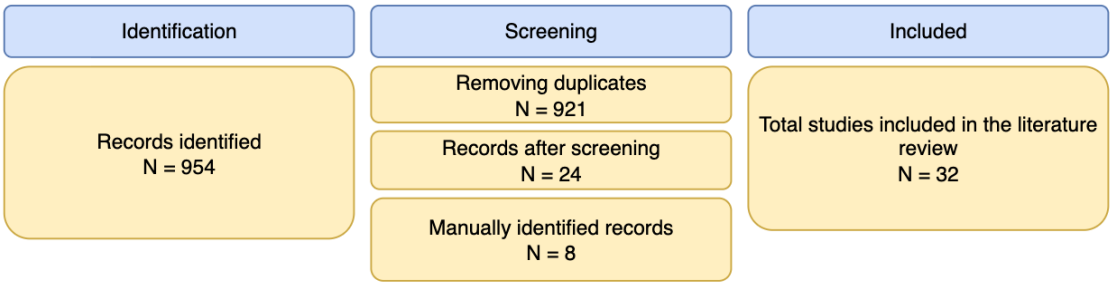

Figure 1. *PRISMA literature review process*

2.2 Review of Existing Research

Bernik presents a study exploring the cybersecurity awareness, practices, and perceptions of Slovenian citizens, aiming to assess how individuals interact with cyberspace and what protective measures they employ [14]. The study uses a descriptive statistical analysis based on a 27-question online survey with 179 respondents. It revealed significant gaps in user awareness and cybersecurity hygiene. Notably, many respondents expressed unjustified confidence in their security while simultaneously failing to implement basic protective measures. For example, only 0.3% reported using fingerprint authentication despite its availability. This research is one of the few attempts to investigate cybersecurity at the citizen level in Slovenia, which marks its relevance. While it claims Slovenia is "comparable to the global average" in cybersecurity, it offers no robust comparative analysis to support this assertion. The study's core finding is that Slovenians are unprepared and undereducated in basic cybersecurity. Importantly, it also critiques the legal and policy environment, noting that cybercrime is easier to commit than to prosecute due to outdated legal frameworks and limited enforcement capacity. This systemic vulnerability strengthens the rationale for population-level research into cybersecurity knowledge and behaviour—precisely what my thesis aims to deliver. My study builds on this foundation with a more representative sample, validated tools, and a deeper analytical framework, offering an updated and more actionable assessment of Slovenia's cybersecurity readiness.

Relating to the previously mentioned study, Slovenia's policy and legal frameworks make cybercrime sometimes difficult to prosecute. As an example of a smaller cybercrime, it is common in Slovenia to download pirated movies. This is likely because internet piracy is not heavily stigmatised in Slovenian society. Economic factors, such as the cost of legal content and the perceived value, also play a role in the decision to access pirated material. In terms of law, Article 148 of Criminal Code states that piracy or the infringement of material copyright is illegal and a criminal offence [15]. This is considering there is a significant financial gain from such infringement. This does not hold for downloading a film or a series. Additionally, someone would have to report you to the police, which does not happen in Slovenia.

The Cyber Security Strategy of the Republic of Slovenia (2016) is a document that sets out to establish a comprehensive national approach to cyber security. However, upon closer inspection, it becomes clear that the strategy is more of a political formality than a robust, actionable framework. For a country facing increasing cyber threats [4], the document's superficial treatment of key issues, lack of concrete data, and over-reliance on vague institutional promises highlight a systemic inadequacy that borders on negligence. The document repeatedly acknowledges that operational capacities are fragmented, underfunded, and lack

both technical and human resources, yet offers no immediate or realistic solution beyond aspirational statements about future improvements [5]. The strategy's so-called vision to achieve a "safe and secure cyberspace" is undermined by the absence of any binding commitments or accountability structures. There is no clear timeline, no performance indicators, and no critical reflection on past failures. Instead, the text relies heavily on buzzwords—"awareness," "coordination," "public-private partnerships"—without addressing how these will be operationalised or monitored. The lack of any cyber security education in primary and secondary schools is mentioned as a weakness, but the response is simply that curricula should include it—eventually. Another example is the reliance on SI-CERT, a small and under-resourced team, to manage a growing volume of incidents [4]. Moreover, while the strategy talks about "raising awareness," it gives no data on the current levels of public knowledge or behaviour. It mentions campaigns like "Safe on the Internet" but offers no evaluation of their effectiveness. The document is a reflection of a reactive, not proactive approach. It highlights the urgent need for research into what Slovenians actually know and do when it comes to cyber security.

Slovenia is currently in the process of transposing the EU NIS2 Directive [16] into national law. The draft legislation, known as the Information Security Act (ZInfV-1), was approved by the Slovenian government in April 2025 and submitted to the National Assembly under an urgent procedure. The law is expected to be adopted by the end of May 2025 [17]. The proposed ZInfV-1 aims to expand the scope of those required to implement cybersecurity measures, encompassing both public and private sectors. Required entities will need to conduct risk assessments and develop cyber incident management plans. The Government Information Security Office (URSIV) will serve as the supervisory authority overseeing compliance with the new regulations [17]. Despite the original transposition deadline of 17 October 2024, Slovenia, along with 22 other EU Member States, failed to meet this requirement. Consequently, the European Commission initiated infringement procedures against these countries [18].

Klein, Zwilling, and Lesjak conducted a comparative study examining cybersecurity awareness, knowledge, and behaviour among students in Israel and Slovenia, with a particular focus on the role of education in shaping protective practices [19]. Their research demonstrates that cybersecurity awareness mediates the relationship between specific knowledge—particularly that gained through formal IT security training—and the adoption of protective behaviours [19]. Specifically, only 21.8% of Slovenian students had attended such training, but those who had scored significantly higher in both awareness and behavioural protection metrics. The mediation model showed that attendance in IT security courses was significantly linked to greater awareness ($\beta = 0.15$, $p < 0.10$), and that awareness in turn was positively associated with cyber protection behaviours

($\beta = .25$, $p < 0.01$). The indirect effect was statistically significant ($B = .11$, $p < 0.001$), confirming that awareness is a key mechanism through which specific training leads to safer behaviour. Notably, Slovenian students exhibited stronger protective behaviour than their Israeli counterparts ($\beta = -.40$, $p < 0.01$), despite reporting similarly moderate levels of self-perceived awareness. While this highlights the importance of targeted educational interventions, the study is constrained by its number of participants (only 35 Slovenian), narrow focus on students from economics and business disciplines, limiting its applicability to the broader Slovenian population. Importantly, the study reveals that general computer knowledge has little impact on cybersecurity behaviour unless accompanied by specialised training. Only participants with IT security course attendance showed significantly higher protective behaviour scores ($M = 5.53$) compared to those without ($M = 4.93$, $p < .05$). This indicates a gap in the effectiveness of general awareness initiatives. By expanding beyond the academic sample and analysing knowledge-behaviour dynamics across various population groups, this thesis offers a more comprehensive understanding of cybersecurity practices in Slovenia.

Velki et al. (2022) conducted a cross-cultural validation of the Behavioural-Cognitive Internet Security Questionnaire in Slovenia [20]. It confirmed that the overall structure of the questionnaire reliably measures the intended psychological constructs (construct validity). However, it noted that some behavioural subscales—such as those assessing password habits or device protection—showed low internal consistency. This indicates that the individual items within those subscales did not consistently measure the same underlying behaviour. Their research provides a validated tool for measuring risky online behaviour and cognitive security awareness but remains narrowly focused on psychometric properties. It lacks a substantive exploration of actual cybersecurity knowledge and behavioural trends across demographics in Slovenia. While the BCISQ captures self-reported and simulated behaviours, the study does not analyse how knowledge levels influence these behaviours, nor does it critically assess cultural or contextual factors impacting security practices.

Bernik, Prislan, and Mihelič conducted a national field study comparing technology use and perceived cybercrime victimisation between rural and urban residents in Slovenia [21]. The study revealed notable differences in the frequency and purpose of ICT use, with urban residents using digital technologies more intensively for activities such as browsing and downloading, yet perceiving higher vulnerability to certain cyber threats, including online shopping scams and social network risks. The study used a novel perspective to find differences in cybersecurity behaviour. The study largely equates "perceived vulnerability" with actual risk, without distinguishing between fear, competence, and real-world exposure. This is a critical limitation, as perceived vulnerability may reflect anxiety or low confidence

rather than genuine exposure to cyber threats, leading to misinterpretation of how secure or at-risk different groups actually are. For instance, someone may feel highly vulnerable due to media influence or low digital self-efficacy, even if they rarely engage in risky online behaviour, while others may underestimate their risk despite engaging in unsafe practices. Overall, it provides some insight into geographical variations, which is valuable for the discussion of this study's findings.

Vrhovec and Markelj explore the cybersecurity awareness of decision-makers in Slovenian organisations, a group often overlooked despite its crucial role in shaping organisational security culture and policy [22]. Using a survey of 283 respondents across executive and non-executive roles, the authors investigated the relationship between awareness of threats and solutions, adoption of security technologies, and various personal and organisational factors. The results reveal very low levels of awareness even among senior decision-makers, particularly non-IT/IS executives. The study is methodologically strong, employing non-parametric tests and robust psychometric analysis. This study confirms that cybersecurity knowledge and behaviour are not adequately addressed even at the highest organisational levels in Slovenia. While the study highlights deficiencies among professionals expected to lead by example, this thesis complements it by focusing rather on the general population.

Mihelič, Bernik, Vrhovec, and Mihelič explore the impact of perceived cyber threats and psychological factors on the adoption of tablet computers among Slovenians aged 65 and older [23]. Using a cross-sectional survey of 119 participants, they categorised respondents into three distinct adoption groups: pre-adoption (individuals considering but not yet using tablets), non-adoption (individuals with no intention of using tablets), and post-adoption (current tablet users). Their regression analysis found that perceived usefulness ($\beta = 0.45$, $p < 0.001$) and existing knowledge ($\beta = 0.38$, $p < 0.01$) were strong predictors of adoption, while anxiety ($\beta = -0.33$, $p < 0.01$) and perceived threat ($\beta = -0.29$, $p < 0.01$) significantly influenced fear of use and rejection of technology benefits. This study offers valuable insight into how cybersecurity perceptions obstruct technology adoption, even when older users are supported by their environment. The research focuses narrowly on tablet use, limiting its applicability to broader cybersecurity behaviour or competence across devices or contexts. For this thesis, it highlights the psychological and emotional barriers to secure digital behaviour among older adults. While their scope is limited to a specific demographic and device, the study complements this thesis by contributing valuable insights into the cybersecurity attitudes of Slovenia's oldest users.

Ilievski and Bernik offer a comprehensive overview of how cybercrime is addressed in Slovenia, focusing on the organisational structure, legal framework, and institutional in-

volvement in combating digital offences [24]. The study examines the roles of national institutions such as the Centre for Computer Investigation, SI-CERT, and various non-police, private, and international bodies, while critically reviewing the legal instruments underpinning Slovenia's cybercrime response—such as the Criminal Code and international conventions. The authors found that Slovenia possesses a relatively advanced legal framework for addressing cybercrime but lacks in efficient enforcement. The gaps are attributed not to legal deficiencies, but to insufficient training, limited technological capabilities, lack of coordination, and the "dark figure" of cybercrime going unreported. This article contributes crucial context to this thesis, particularly in demonstrating that institutional and legal structures alone are not sufficient to ensure cybersecurity. Where Ilievski and Bernik focus on system-level failures, this research targets the individual-level knowledge and behaviour, complementing the policy intentions with the population's actual digital experience. This thesis will help inform where strategic awareness and education efforts might actually make a difference.

In a 2020 interview with the Slovenian Press Agency, then Police Commissioner Tatjana Bobnar highlighted the growing challenges posed by cybercrime in Slovenia [25]. She emphasised that while the police have made improvements in establishing cybercrime divisions and acquiring forensic tools, they are hindered by legal limitations, particularly in monitoring encrypted communications and using technologies like IMSI catchers and automatic licence plate recognition. Bobnar called for legislative reforms to enhance the police's capabilities in combating cyber threats, highlighting the importance of balancing privacy rights with public safety. This article provides valuable insight into the complexities of cybercrime legislation and enforcement in Slovenia. For this thesis, it highlights the critical need for updated legal frameworks to effectively combat cybercrime.

Markelj and Zgaga conducted an empirical study exploring Slovenian university students' awareness of cyber threat [26]. Their survey revealed a paradoxical situation: students were partially aware of traditional threats like theft and viruses but poorly informed about newer or more sophisticated risks, such as malware infection, phishing, or rootkits. Most participants also lacked familiarity with essential protective measures, including PIN protection for apps, VPN use, or remote data deletion. This research makes two valuable contributions. First, it highlights user ignorance and overconfidence, which lead to riskier behaviour. Second, it shows that the user may be held responsible for consequences they do not even understand or anticipate, especially if organisational policy formally required protective conduct. Where the study illustrates the legal implications of ignorance, this thesis seeks to measure that ignorance and find potential demographic patterns.

Blažič and Cigoj present a European study investigating the relationship between

population-level digital skills and the security of web services [27]. Using their custom vulnerability-scanning tool (Vulnet), they inspected over 3.7 million European websites and correlated detected vulnerabilities with digital skills indexes, internet infrastructure costs, and socio-economic indicators. Their findings demonstrate a statistically significant relationship: countries with higher digital skills and more affordable internet infrastructure show fewer insecure websites, both in general and within key sectors such as education, finance, and healthcare. The study's biggest strength is its wide scope, comparing multiple European countries. However, it evaluates security at the infrastructure level, not personal like this thesis does but it provides some valuable insight. Slovenia is placed among the countries with a high proportion of insecure websites and only moderate digital skills. This raises concerns and supports the urgency of further research in this context. For this thesis, it provides a macro-level context, which the thesis will complement with micro-level research of citizens' knowledge and behaviour.

Šolić, Idlbek, and Velki conducted an empirical study comparing users' self-assessed cybersecurity behaviour to their objectively measured risk using the BCISQ questionnaire on a sample of 278 university students [28]. Through simulated behavioural tasks—including trick questions on password disclosure and terms-of-service reading—the study found that those who engaged in riskier behaviour were more likely to believe they were behaving securely, a contradiction that underscores a significant cognitive bias in self-assessment. Their findings show that over 22% of students revealed a real password, and almost 90% failed to read consent conditions, despite believing their behaviour was secure. These results expose gaps between perceived and actual security behaviour and raise concerns about overconfidence and habitual risky practices. Although the study offers a methodologically detailed analysis, it does not account for broader demographics or national representativeness. Their findings are insightful and closely related to this thesis. However, this thesis will extend this work by researching on a more representative sample of Slovenians and evaluating how demographic, educational and contextual factors influence personal cybersecurity knowledge and behaviour.

Several studies in the literature review emphasise that personal cybersecurity research must adopt a tailored approach, due to the variability of human behaviour—even within the same demographic group. For example, Sangwan (2024) and Douha (2023) show that individual psychological traits such as risk tolerance, stress response, and decision-making styles significantly influence security behaviour, suggesting that generic awareness campaigns often fail to engage diverse user needs [29, 30]. Taylor-Jackson (2020) and Mashiane (2019) argue that education efforts must be adapted based on learning preferences and emotional engagement, rather than assuming a uniform audience [31, 32]. Other studies point to specific vulnerabilities, such as those related to neurodiversity or cognitive overload, as

highlighted by Kohler (2023) and Sutterlin (2023) [33, 34]. Although these studies are not set in the Slovenian context, they provide critical theoretical support for the need to assess Slovenian cybersecurity knowledge and behaviour in a similar and population-specific manner.

Owen, Flowerday, and van der Schyff examine the role of optimism bias—a cognitive bias leading individuals to underestimate personal risk—in influencing phishing susceptibility [35]. They analysed 226 survey responses from a South African financial services organisation using partial least squares modelling. Their findings demonstrate that employees with higher optimism bias are significantly less likely to engage in secure behaviour, mainly due to overconfidence in their immunity to threats and misplaced trust in technical defences. While the study's contribution to understanding psychological vulnerabilities in cybersecurity is notable, several limitations reduce its direct applicability to a broader context. The sample is restricted to a single organisation and cultural setting, limiting external validity. However, it was included in this review because it offers a valuable psychological insight (optimism bias) that is globally relevant, particularly in relation to phishing. Furthermore, although the study successfully integrates optimism bias into behavioural models, it does not explore demographic variations or general cybersecurity knowledge levels.

Sturman, Bell, Auton, Breakey, and Wiggins investigated how phishing knowledge, cue utilization, and decision styles influence the ability to detect phishing emails [36]. The study sampled 145 Australian adults (M = 52.8 years). It found that cue utilisation (the ability to recognise meaningful features quickly) was the only variable that independently predicted phishing detection accuracy, with a statistically significant effect ($\beta = 0.48$, $p < .001$), while phishing knowledge ($\beta = 0.18$, $p = .064$) and decision style ($\beta = -0.08$, $p = .260$) did not significantly contribute to the predictive model. In contrast, phishing knowledge mainly led to increased caution (bias towards classifying emails as phishing) rather than true detection skills, and intuitive decision-making styles correlated with poorer performance. While methodologically rigorous, the study's focus on a non-Slovenian sample and controlled laboratory settings with forced exposure times limits its direct applicability. Nevertheless, it was included because it provides a robust, generalisable framework for understanding the cognitive mechanisms behind phishing detection. These mechanisms remain highly relevant in the Slovenian context where such cognitive processing patterns have not yet been empirically studied.

Chowdhury, Adam, and Skinner conducted a systematic review of 21 empirical studies to investigate how time pressure influences cybersecurity behaviour [37]. Their work is notable for synthesising findings into an integrative framework, which categorises time pressure effects into three pathways: cognitive overload, which impairs users' ability to

assess risk; reliance on habitual or intuitive decision-making, which increases susceptibility to threats; and diminished attention to security cues, such as warnings or authentication steps. It highlights a concerning gap: most existing studies focus on intentions rather than actual behaviour, and many rely on self-reports, opening the door to biases like social desirability and recall inaccuracies. This gap between intentions and behaviour is critical because users often report that they would act securely under time pressure, but behavioural data shows that in practice, they tend to skip security steps, such as ignoring warnings or reusing passwords, due to stress or urgency. This discrepancy demonstrates the need for empirical data on what users actually do, not just what they say they intend to do, which this thesis directly addresses. Moreover, most of the reviewed studies simulate time pressure through hypothetical scenarios rather than real-world conditions, which limits validity. For this study, this review reinforces the importance of considering real behavioural outcomes. While time pressure is not a direct focus of this work, understanding that everyday pressures negatively affect risky behaviour should be considered. Their findings further highlight that addressing cybersecurity cannot rely solely on technical solutions or policy. It requires accounting for human limitations under realistic pressures.

Dupuis, Geiger, Slayton, and Dewing conducted a large-scale survey (n = 1,002) examining why consumers adopt or reject various cybersecurity tools—including anti-malware software, password managers, VPNs, backups, and two-factor authentication—and whether they desire access to expert help [38]. The study found that the adoption of these tools varies widely by age and gender, with younger users generally adopting more tools, and that self-efficacy plays a crucial role in security behaviour. Many users cite perceived complexity, lack of knowledge, and cost as barriers. Although the paper effectively identifies usability barriers, it fails to contextualise these behaviours within broader frameworks of digital literacy, cultural context, or formal knowledge assessment. This work highlights that tool non-use is not due to ignorance alone, but also to low confidence in one's ability to use cybersecurity tools effectively and a lack of perceived control over security outcomes. For example, users may feel that even with a password manager or VPN, they remain vulnerable.

Obar and Oeldorf-Hirsch conducted a large-scale experimental survey to empirically demonstrate that most users do not read privacy policies or terms of service, even when confronted with absurd and invasive clauses [39]. In their study of 543 undergraduate participants, 74% accepted a fictitious social media platform's policies without viewing them, and 98% failed to notice "gotcha" clauses including data sharing with the NSA or the surrender of one's first-born child. Median reading times were as low as 14 seconds for policies requiring 30 minutes or more to read in full. This study delivers strong empirical support for the argument that notice and choice frameworks are fundamentally

broken. Even participants studying communication and privacy at university, who are likely more informed than the general public, routinely ignored critical consent material. The authors uncover reasons ranging from information overload to resignation and cultural normalisation of non-reading. This confirms the privacy paradox: a phenomenon where individuals express strong concern for privacy in principle but fail to take actions that protect it in practice. Although the study is highly insightful, it is constrained to a very specific behaviour (policy reading) and a narrowly defined sample (students). This limits its scope for policymaking beyond critique of legal consent norms.

Cravens and Resch (2023) investigated the password hygiene between 74 Computer Science (CS) and 45 non-CS undergraduates [40]. While CS students demonstrated only marginally better knowledge based on a modified Pew Research survey, their password hygiene was significantly superior. This included greater use of random elements, longer passwords, higher rates of password manager adoption, and more consistent use of two-factor authentication. The study shows that knowledge alone does not predict secure behaviour. This finding is particularly relevant for this thesis, as it supports the view that cybersecurity competence is not only a function of theoretical understanding, but also of behavioural habits.

Kankane, DiRusso, and Buckley conducted an online experiment to explore whether behavioural nudges could encourage better password management behaviour [41]. Nudges are subtle design interventions intended to steer users toward more desirable behaviours without restricting their choices. Using five types of nudges—salience (highlighting importance), norm (indicating what others do), incentive, ego (appealing to self-image), and default—the researchers tested their influence on 263 participants' comfort with auto-generated passwords and their willingness to change them. The salience nudge, which used emotionally charged, fear-based language, was the only one to significantly reduce users' comfort with insecure password defaults. However, none of the nudges significantly altered actual password-changing behaviour, revealing a persistent gap between intention and action. It highlights the limitations of relying solely on interface design to compensate for poor cybersecurity habits, without addressing the foundational knowledge deficits this thesis aims to discover.

Taylor-Jackson, McAlaney, Foster, Bello, Maurushat, and Dale propose an educational framework for enhancing cybersecurity awareness through the integration of psychological principles [31]. The paper argues that most existing cybersecurity training efforts are overly technical and fail to account for cognitive, behavioural, and emotional dimensions of user decision-making. By applying psychological theories, specifically the Theory of Planned Behaviour (which explains how intention, perceived behavioural control, and attitudes

influence action) and Protection Motivation Theory (which focuses on how perceived severity, vulnerability, response efficacy, and self-efficacy shape protective behaviours), the authors aim to improve not only what users know, but how they internalise and apply cybersecurity knowledge. The paper's strength is in its interdisciplinarity, blending psychology with cybersecurity education. It provides valuable theoretical support for the idea that cybersecurity knowledge must be contextually embedded and psychologically resonant to be effective.

Sámson and Tick explore the human factor of cybersecurity by comparing information security awareness in professional and personal contexts through a quantitative survey of 244 respondents [42]. The study investigates behavioural practices such as password reuse, public Wi-Fi use, and response to potential threats, while also analysing the impact of demographic factors, workplace training, and self-initiated education. The study's main contribution is its identification that self-education is a stronger predictor of secure behaviour than formal workplace training, especially in personal contexts. Moreover, the study supports the view that the human factor is the weakest link in information security. Demographic variables such as gender and generation had negligible influence on awareness. The study is limited by a strong focus on awareness rather than actual competence. The research supports this thesis by reaffirming the critical gap between cybersecurity knowledge and actual behaviour, especially in private life. Additionally, it indicates that encouraging self-initiated education might be more effective than traditional education.

Snyman and Kruger introduce the concept of information deserts—areas within organisations or communities where information flow is structurally restricted [43]. The authors argue that cybersecurity campaigns fail not only due to content or frequency, but because contextual environmental factors limit the reach and absorption of security knowledge. Their findings show that even well-designed awareness efforts are likely to fail if delivered in environments that restrict information exchange. However, the research is primarily theoretical and illustrative, lacking quantitative validation or behavioural outcome measurement. The analysis is context-specific and cannot be generalised across different sectors or populations. The paper supports this thesis by emphasising that information access alone does not equate to cybersecurity awareness or secure behaviour.

2.3 Definition of Key Terms

Self-Efficacy and Cybersecurity

Numerous studies highlight that individuals' cybersecurity practices are not only influenced by their technical knowledge but also by psychological and behavioural factors such as self-efficacy. Self-efficacy is an individual's belief in their ability to execute specific tasks successfully [11]. This psychological construct plays an important role in determining how individuals perceive their ability to navigate and mitigate risks, especially in the context of cybersecurity. Individuals must feel confident in their capacity to recognise, respond to, and mitigate such risks.

Research consistently demonstrates that self-efficacy is a key predictor of cybersecurity behaviour. For instance, high levels of self-efficacy are linked to proactive security practices such as adhering to security protocols, reporting suspicious activity, and engaging in continuous training to stay up-to-date with evolving threats [44]. In contrast, individuals with low self-efficacy may feel overwhelmed or powerless when dealing with cyber threats, which leads to avoidance behaviours, errors, or an over-reliance on colleagues or technological solutions [45]. This lack of confidence in the ability to handle cyber risks may ultimately lead to increased vulnerabilities.

Self-efficacy can be influenced by external factors such as training, feedback, and the perceived support from organisational structures. A positive reinforcement environment, where individuals receive consistent feedback on their security practices, has been shown to enhance self-efficacy and therefore security behaviours [46]. Likewise, a lack of support or training can cause feelings of helplessness and incompetence, leading to lower engagement with security practices.

The importance of improving self-efficacy is also highlighted in the context of social engineering, where attackers exploit human psychological weaknesses rather than technical vulnerabilities. Individuals with low self-efficacy may be more susceptible to manipulation in phishing and other social engineering tactics, which further shows the need for attention on psychological cybersecurity training [47].

The integration of self-efficacy into cybersecurity practices is part of human factors in cybersecurity, which is an essential component [46]. By addressing the psychological factors that influence individual behaviours, exposure to cyber threats that proceed from these factors could be reduced. This would cultivate a more resilient cybersecurity culture.

Cybersecurity Knowledge

Cybersecurity knowledge refers to an individual's understanding of digital threats, protection mechanisms, and best practices in maintaining security in online environments. This includes familiarity with phishing, malware, password hygiene, multi-factor authentication, and safe browsing practices. Several studies show that while many users overestimate their knowledge, actual understanding is often limited, especially in the Slovenian context [26, 19, 20]. In Klein et al.'s comparative study, general computer literacy had little impact on behaviour unless supported by specific cybersecurity training [19]. Similarly, Markelj and Zgaga found that university students lacked knowledge about sophisticated threats like rootkits or phishing [26]. Accurate cybersecurity knowledge is essential for informed decision-making, yet literature shows that awareness alone is insufficient without verified comprehension and application. Therefore, measuring and contextualising this knowledge is a critical aspect of this thesis.

Cybersecurity Behaviour Gap

The cybersecurity behaviour gap refers to the discrepancy between what individuals know about cybersecurity and how they act in practice. While individuals may express awareness of digital risks, studies repeatedly reveal inconsistencies between knowledge and behaviour [28, 39, 38]. For instance, users who claim to care about privacy often ignore privacy policies—a phenomenon termed the "privacy paradox" [39]. Similarly, in behavioural experiments using the BCISQ, students disclosed real passwords despite claiming secure habits [28]. This gap is further widened by overconfidence, social desirability bias, and reliance on habitual responses, which are worsened under time pressure. Specifically, users may resort to intuitive, automatic (System 1) thinking rather than deliberate, reflective (System 2) processing, especially when faced with stress, urgency, or task interruptions. Under such conditions, individuals are more likely to prioritise speed over accuracy, trust superficial cues, or ignore security protocols in favour of completing primary tasks efficiently [37]. In the Slovenian context, such inconsistencies have been noted in both student and older adult populations, where self-perceived cybersecurity competence does not match real-world behaviour [14, 23]. Recognising and analysing this gap is central to understanding the limits of awareness campaigns and training programmes, and it forms a crucial part of this thesis' contribution.

2.4 Research Questions: Preliminary Findings from Literature

Based on the systematic literature review, research questions can be provisionally addressed. The review analysed both Slovenian and international studies, providing context, empirical findings, and methodological insights. Below are the preliminary findings based on the

literature review:

1. **MRQ: What is the current state of cybersecurity knowledge and behaviour among Slovenians?**
   Based on the literature review, the current state of cybersecurity knowledge and behaviour among Slovenians is concerning and marked by several contradictions. Multiple studies, including Bernik's early research [14] and more recent investigations [26, 48], revealed that Slovenians exhibit low practical cybersecurity knowledge despite a high self-perception of safety. There is a repeating pattern of overconfidence, minimal adoption of protective measures, and widespread use of insecure practices such as password reuse or neglecting updates [14, 40].
   The literature also suggests a persistent gap between knowledge and behaviour. For example, while participants often claim to understand privacy or phishing risks, they consistently fail to recognise threats or act securely in practice, as shown in behavioural simulations [28, 36]. Furthermore, the Slovenian national strategy [5] provides no empirical data on population-level awareness or practices, which further shows the necessity of this thesis.
   Comparatively, findings from non-Slovenian studies reveal similar trends, such as the global phenomenon of the "privacy paradox" [39] or the ineffectiveness of nudges without deeper cognitive engagement [41]. However, these studies were conducted within different cultural and infrastructural contexts, making direct comparisons with Slovenia methodologically limited. Nonetheless, they reinforce the relevance of this national-level research.
2. **SRQ1: What is the level of self-efficacy for information security among Slovenians?**
   The literature review reveals limited direct data on Slovenian self-efficacy in cybersecurity. However, indirect findings suggest it is likely overestimated. Bernik's and Markelj's research both show a mismatch between perceived and actual capability, especially among students and older adults [14, 26, 23]. Similarly, international studies find that individuals' self-perceptions do not reliably predict their security actions [28, 48]. Dupuis et al. additionally highlight that low self-efficacy acts as a barrier to adopting security tools [38]. The thesis will use the SEIS scale to directly measure self-efficacy of Slovenians.
3. **SRQ2: What is the level of cybersecurity knowledge among Slovenians?**
   The literature review found that Slovenian users demonstrate only partial or outdated cybersecurity knowledge, often lacking awareness of modern threats such as rootkits, phishing techniques, or secure authentication practices [26, 27]. Klein et al.'s study comparing Slovenian and Israeli students showed that cybersecurity knowledge among Slovenians was limited to what was gained through targeted IT training,

while general computer literacy had no real behavioural impact [19].

Moreover, educational strategies in Slovenia remain underdeveloped. The national strategy admits the absence of cybersecurity education in schools [5], and most campaigns have unevaluated effectiveness. Some users, particularly older adults, are hindered not only by knowledge gaps but also by fear and anxiety associated with digital risks [23]. The Slovenian cybersecurity knowledge appears to be fragmented, context-dependent, and largely untested, which supports the necessity of this thesis' knowledge survey.

4. **SRQ3: What are the actual cybersecurity behaviours of Slovenians?**

   Based on the literature review, the behaviours identified among Slovenians include poor password hygiene, infrequent use of two-factor authentication, limited awareness of software update practices, and a tendency to rely on basic, often outdated, forms of protection (e.g. antivirus software alone) [14, 40, 28]. Even those with higher knowledge levels do not seem to translate it to safer behaviour. For example, they may express concern about phishing or privacy but still engage in unsafe practices like ignoring Terms of Service or clicking suspicious links [39, 36].

   Behavioural findings from Slovenian studies are scarce and non-generalisable, often relying on student populations. International literature confirms that real-world behaviour is shaped more by habit, time pressure, interface design, and emotional factors than by abstract knowledge alone [37, 42]. This thesis will address the research gap by measuring scoring cybersecurity behaviours of Slovenians across demographics. This will help distinguish knowledge from behaviour and offer realistic insights.

3. Research Methodology

3.1 Subjects

An online survey was distributed to several universities, organisations, and companies. The research collected $n = 164$ responses. Five responses were left blank, and were therefore excluded from the analysis.
To calculate the number of participants needed for the research to detect a real effect, if one truly exists, a power analysis was done. Using the Statistical Power Analysis tool G*Power [49], the power was set to 0.95 (95%) with an expected medium effect size ($f^2 = 0.15$), and it was calculated that for most tests, the number of responses needed ranges from 100 to 140. This means that $n = 164$ is well above the required minimum. The participants are Slovenians aged 18 and over, meaning parental consent was not required. They represent diverse demographic groups in terms of educational background, age, gender, field of work, and perceived expertise.

3.2 Instruments

The data collection instrument chosen for this research was Google Forms survey administration software [50]. Google Forms was selected as the data collection platform due to its accessibility, ease of use, and suitability for academic research. It allows for efficient dissemination of surveys to large numbers of participants while enabling standardisation of question formats and automatic collection of responses in a structured and exportable format. This facilitated both the management of the data and its subsequent analysis. In the context of a master's thesis, Google Forms represents an appropriate and pragmatic tool for data collection. It supports the ethical requirements of informed consent, anonymity, and voluntary participation, all of which were incorporated into the design of the questionnaire. To ensure compliance with the GDPR, specific settings within Google Forms were configured: the collection of email addresses was disabled, participants were not required to log in with a Google account, and responses were gathered anonymously. Participants were also informed about the purpose of data collection, their right to withdraw, and how their data would be stored and used, in line with GDPR principles [51, 52]. Moreover, the platform's compatibility with spreadsheet software allows for seamless integration with data analysis tools, making it well suited for empirical, quantitative research within academic settings. The online format also allows participants to complete the questionnaire at their convenience, potentially improving response rates and the quality of responses.

The questionnaire is divided into four distinct sections, each targeting a specific aspect of the research framework. The first section employs the Self-Efficacy for Information Security (SEIS) scale, a validated instrument that assesses participants' confidence in their ability to protect personal digital information. It consists of eleven questions and uses a 7-point Likert scale. Higher number means stronger agreement with the statement and lower number stronger disagreement. It is expected that people who score higher on the SEIS scale are better at cybersecurity. Measuring self-efficacy is critical to understanding the psychological factors that may influence security-related behaviours.
The second section tests the General Controllability (GEI) scale, consisting of three items that evaluate the extent to which individuals generally perceive their cybersecurity outcomes to be within control. It uses the same 7-point Likert scale, same as SEIS.
The third section assesses cybersecurity knowledge through a series of test-like items. These items are designed to evaluate participants' understanding of fundamental cybersecurity concepts and practices, such as password security, phishing detection, and the use of multi-factor authentication. This component serves to gauge the actual level of cybersecurity literacy within the sample population. Each answer is scored with either 0, 1 or 2 points. At the end, the total score is calculated which allows for empirical analysis of individuals' knowledge level.
The final section explores the cybersecurity habits and behaviours of respondents. Questions in this section are aligned with best practice recommendations and address routine security activities such as software updates, password management, and responses to suspicious digital content. The findings from this section directly inform the research subquestion regarding real-world cybersecurity behaviours. This section is also graded, with each answer receiving 0, 1 or 2 points, ranging from riskiest (0 points) to safest (2 points). The total score allows for empirical analysis to compare how risky each participants' real-world behaviour is.

Together, these four sections provide a comprehensive data set that captures the interplay between perceived confidence, perceived control, actual knowledge, and behavioural practices in cybersecurity. The inclusion of standardised scales (SEIS and GEI), combined with test-like knowledge and behaviour items, ensures that the research questions are addressed systematically and robustly. The chosen design also supports the identification of potential gaps between individuals' perceived and actual cybersecurity competence, aligning with the goals of the study. Grading the answers allows for empirical analysis, making it easier to demonstrate the findings.

3.3 Procedure

Data for this research were collected using a structured online questionnaire on Google Forms. The decision to do an online survey was made because of the study's objective to obtain a broad and diverse sample of participants from across Slovenia. The questionnaire was distributed through multiple channels, including university mailing lists, professional and academic networks, corporate contacts, and informal social circles such as friend groups. This strategy ensured accessibility and reach across a variety of demographic and occupational backgrounds, enhancing the diversity and potential representativeness of the sample. The responses were collected between March and April 2025, until a sufficient number of responses were gathered and all contacts were used.
The data collected was exported into spreadsheet format for further processing and analysis. The raw responses include both structured quantitative items—such as Likert-scale responses from the SEIS and GEI instruments—and open-ended responses assessing cybersecurity knowledge and behavioural habits.

This research adhered to established ethical standards for conducting human-centred studies, with particular attention to data privacy, informed consent, and voluntary participation. All participants were required to provide informed consent before proceeding with the questionnaire. The consent form clearly stated that participation was entirely voluntary, that responses would remain anonymous, and that the data would be used solely for research purposes. The setting for collecting email addresses was set to "Do not collect". Participants were also informed that their data would be securely stored, accessible only to the researcher, and permanently deleted upon completion of the analysis.
To further safeguard participant confidentiality and comply with ethical norms and GDPR, no personally identifiable information was collected at any stage of the research. The study design ensured that participants could withdraw at any point by simply choosing not to continue. These measures reflect ethical integrity and align with the requirements of academic research.

4. Data Analysis and Results

4.1 Overview of the Chapter

This chapter presents the results of the statistical analyses conducted on the survey data from 164 participants. Shapiro-Wilk test revealed non-normality of several variables. Therefore, appropriate non-parametric tests were used alongside parametric procedures. The analyses included Spearman's rank-order correlations, Mann–Whitney U tests, one-way ANOVAs with post hoc comparisons, linear regressions, and a mediation analysis. Key variables examined were cybersecurity self-efficacy (SEIS), general expertise (GEI), cybersecurity knowledge, and cybersecurity behaviour. These were analysed in relation to gender, education level, and perceived expertise. The chapter explores associations between these variables, differences across groups, and predictors of behaviour and knowledge, with all analyses conducted using JASP tool (Version 0.19.3) [53] and reported in accordance with the official JASP statistical manual [54].

4.2 Demographic Distribution of Respondents

This part of the analysis provides an overview of the categorical demographic variables collected in the survey: gender, education level, and perceived cybersecurity expertise. Frequency distributions are presented for each variable to describe the composition of the sample.

Table 1. Descriptive statistics for categorical demographic variables

	Valid	Missing	Mean	Std. Deviation	Minimum	Maximum
Gender	164	0				
Education	164	0				
Perceived expertise	164	0	2.287	0.977	1.000	4.000

- **Gender:** The majority of respondents were female (65.2%), while males represented 34.8%. No responses were missing.

Table 2. Gender Frequency Table

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Female	107	65.244	65.244	65.244
Male	57	34.756	34.756	100.000
Missing	0	0.000		
Total	164	100.000		

- **Education:** Participants held various levels of education. The largest group had a bachelor's degree (36.6%), followed by master's degree (26.2%), secondary school graduates (20.7%), and those with doctoral degrees (16.5%).

Table 3. Education Frequency Table

Education	Frequency	Percent	Valid Percent	Cumulative Percent
Bachelor's degree	60	36.585	36.585	36.585
Doctoral degree	27	16.463	16.463	53.049
Master's degree	43	26.220	26.220	79.268
Secondary school	34	20.732	20.732	100.000
Missing	0	0.000		
Total	164	100.000		

- **Perceived Expertise:** Respondents self-assessed their cybersecurity knowledge on a four-level scale. The most common category was Advanced (40.2%), followed by Novice (28.7%), Intermediate (22.6%), and Expert (8.5%).

Table 4. Frequencies for Perceived expertise

Perceived expertise	Frequency	Percent	Valid Percent	Cumulative Percent
Novice	47	28.659	28.659	28.659
Intermediate	37	22.561	22.561	51.220
Advanced	66	40.244	40.244	91.463
Expert	14	8.537	8.537	100.000
Missing	0	0.000		
Total	164	100.000		

These distributions help contextualise the subsequent analyses and ensure that key demographic groups are represented in the sample. This is important when comparing cybersecurity knowledge, behaviour, and self-efficacy across different subgroups later in the chapter.

4.3 Data Normality

To determine the appropriate statistical tests for further analysis, the Shapiro–Wilk test was conducted to assess the normality of the main variables: age, SEIS score, GEI score, total knowledge score, and total behaviour score. As shown in the table 5, all variables violated the assumption of normality, with Shapiro–Wilk p-values below the standard significance threshold of 0.05. This indicates that the data distributions are significantly different from normal. Therefore, non-parametric statistical tests will be applied throughout the analysis to ensure valid results.

Table 5. Shapiro-Wilk Test

	Mean	Std. Deviation	Shapiro-Wilk	P-value of Shapiro-Wilk	Minimum	Maximum
Age	35.030	14.027	0.884	$<$ .001	19.000	73.000
SEIS SCORE	4.029	1.379	0.979	0.014	1.182	7.000
GEI SCORE	4.230	1.166	0.977	0.007	1.000	7.000
Total score (knowledge, out of 34)	15.183	7.765	0.980	0.018	0.000	31.000
Total score (behaviour, out of 36)	21.774	5.137	0.971	0.002	0.000	31.000

4.4 Correlation Analysis

A Spearman's rank-order correlation was conducted to examine the relationships between self-efficacy (SEIS score), general controllability (GEI score), cybersecurity knowledge, and behaviour. This non-parametric test was selected due to prior results of non-normality in the dataset, confirmed by the Shapiro–Wilk test (see Table 5.

The results are summarised in Table 6. The analysis revealed a moderate positive correlation between self-efficacy and cybersecurity knowledge ($\rho = .525$, $p < .001$), indicating that higher self-reported confidence is associated with greater factual knowledge. A weak positive correlation was observed between self-efficacy and cybersecurity behaviour ($\rho = .311$, $p < .001$), suggesting that higher confidence is linked to somewhat safer online practices. GEI score was moderately associated with SEIS ($\rho = .368$, $p < .001$) and weakly correlated with knowledge ($\rho = .214$, $p = .006$), but not significantly related to behaviour ($\rho = .119$, $p = .130$). Age showed a weak negative correlation with GEI score ($\rho = \breve{}.161$, $p = .039$), suggesting that older participants may perceive slightly less control over cybersecurity outcomes, although it did not significantly relate to SEIS, knowledge, or behaviour.

Table 6. Spearman's Correlations

Variable		Age	SEIS SCORE	GEI SCORE	Total score (knowledge, out of 34)	Total score (behaviour, out of 36)
1. Age	Spearman's rho	–				
	p-value	–				
2. SEIS SCORE	Spearman's rho	−0.003	–			
	p-value	0.971	–			
3. GEI SCORE	Spearman's rho	−0.161	0.368	–		
	p-value	0.039	< .001	–		
4. Total score (knowledge, out of 34)	Spearman's rho	0.087	0.525	0.214	–	
	p-value	0.269	< .001	0.006	–	
5. Total score (behaviour, out of 36)	Spearman's rho	0.052	0.311	0.119	0.498	–
	p-value	0.506	< .001	0.130	< .001	–

These findings indicate that mainly self-efficacy is meaningfully related to cybersecurity knowledge and, to a lesser extent, behaviour.

4.5 Gender Differences in Self-Efficacy, Controllability, Knowledge, and Behaviour

To determine whether there were statistically significant differences between males and females in self-efficacy (SEIS), general controllability (GEI), cybersecurity knowledge, and behaviour, Mann–Whitney U tests were conducted. This non-parametric test is appropriate for comparing two independent groups when the assumption of normality is violated, as confirmed earlier using the Shapiro–Wilk test (Table 5). The Mann–Whitney test compares median ranks between groups and provides a test statistic (U), a p-value, and a rank-biserial correlation as a measure of effect size.

SEIS Score: A statistically significant difference was found in self-efficacy between genders, $U = 1240.000$, $p < .001$. Males had higher mean ranks (114.246) compared to females (65.589), indicating that men rated their self-efficacy higher. The rank-biserial correlation was -0.593, reflecting a large effect size.

GEI Score: No significant difference was observed in perceived general controllability, $U = 2699.500$, $p = .224$. The mean ranks for males (88.640) and females (79.229) were similar, and the effect size was small ($r_B = -0.115$).

Cybersecurity Knowledge (total score out of 34): A significant difference was found between genders, $U = 1782.000$, $p < .001$. Males again had higher mean ranks (104.737) compared to females (70.654), and the rank-biserial correlation was -0.416, indicating a moderate effect.

Cybersecurity Behaviour (total score out of 36): No significant difference was found between groups, $U = 2794.500$, $p = .379$. Mean ranks were similar for males (86.974) and females (80.117), with a negligible effect size ($r_B = -0.084$).

Table 7. Independent Samples T-Test - Gender

	U	df	p	Rank-Biserial Correlation	SE Rank-Biserial Correlation
SEIS SCORE	1240.000		< .001	−0.593	0.095
GEI SCORE	2699.500		0.224	−0.115	0.095
Total score (knowledge, out of 34)	1782.000		< .001	−0.416	0.095
Total score (behaviour, out of 36)	2794.500		0.379	−0.084	0.095

Table 8. Group Descriptives - Gender

	Group	N	Mean	SD	SE	Coefficient of variation	Mean Rank	Sum Rank
SEIS SCORE	Female	107	3.535	1.194	0.115	0.338	65.589	7018.000
	Male	57	4.956	1.224	0.162	0.247	114.246	6512.000
GEI SCORE	Female	107	4.140	1.160	0.112	0.280	79.229	8477.500
	Male	57	4.398	1.169	0.155	0.266	88.640	5052.500
Total score (knowledge, out of 34)	Female	107	13.178	7.376	0.713	0.560	70.654	7560.000
	Male	57	18.947	7.100	0.940	0.375	104.737	5970.000
Total score (behaviour, out of 36)	Female	107	21.579	4.853	0.469	0.225	80.117	8572.500
	Male	57	22.140	5.658	0.749	0.256	86.974	4957.500

4.6 Educational Differences

An ANOVA test was performed to investigate education level has an effect on SEIS, GEI, cybersecurity knowledge, and behaviour. The independent variable was education (four levels: secondary school, bachelor's degree, master's degree, and doctoral degree), and the dependent variables were SEIS, GEI, cybersecurity knowledge, and behaviour scores. Omega squared (ω^2) was reported as a measure of effect size, and post hoc comparisons were conducted using Tukey's HSD and Dunnett's tests.

4.6.1 Educational Differences in SEIS

The results showed no statistically significant differences in SEIS scores across education levels, $F(3, 160) = 2.275$, $p = .082$, with a small effect size ($\omega^2 = 0.023$). Descriptive statistics indicated that mean SEIS scores were slightly higher for participants with doctoral ($M = 4.207$, $SD = 1.391$), bachelor's ($M = 4.171$, $SD = 1.493$), and master's degrees ($M = 4.148$, $SD = 1.314$) compared to those with only secondary education ($M = 3.487$, $SD = 1.142$).

Table 9. ANOVA - Education and SEIS

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Education	12.684	3	4.228	2.275	0.082	0.023
Residuals	297.335	160	1.858			

Table 10. Descriptives - Education and SEIS

Education	N	Mean	SD	SE	Coefficient of variation
Bachelor's degree	60	4.171	1.493	0.193	0.358
Doctoral degree	27	4.207	1.391	0.268	0.331
Master's degree	43	4.148	1.314	0.200	0.317
Secondary school	34	3.487	1.142	0.196	0.327

Table 11. Kruskal-Wallis Test - Education and SEIS

Factor	Statistic	df	p
Education	6.859	3	0.077

Although the overall ANOVA was not statistically significant, post hoc comparisons were examined for completeness. Tukey's HSD test (Table 27) indicated that none of the pairwise differences were statistically significant, though the comparison between bachelor's degree and secondary school approached significance ($p = .093$, $d = 0.502$). Dunnett's post hoc test (Table 13), comparing each group against the bachelor's degree reference, similarly revealed no significant differences, with the contrast between secondary school and bachelor's degree being $p = .057$.

Table 12. Standard HSD Post Hoc Comparisons - Education and SEIS

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Bachelor's degree	Doctoral degree	−0.036	0.316	160	−0.114	−0.026	0.999
	Master's degree	0.024	0.272	160	0.087	0.017	1.000
	Secondary school	0.685	0.293	160	2.340	0.502	0.093
Doctoral degree	Master's degree	0.060	0.335	160	0.178	0.044	0.998
	Secondary school	0.721	0.351	160	2.051	0.529	0.174
Master's degree	Secondary school	0.661	0.313	160	2.113	0.485	0.153

Table 13. Dunnett Post Hoc Comparisons - Education and SEIS

Comparison	Mean Difference	SE	t	$p_{dunnett}$
Doctoral degree - Bachelor's degree	0.036	0.316	0.114	0.999
Master's degree - Bachelor's degree	−0.024	0.272	−0.087	1.000
Secondary school - Bachelor's degree	−0.685	0.293	−2.340	0.057

4.6.2 Educational Differences in GEI

The results revealed no statistically significant differences in GEI scores across the education groups, $F(3, 160) = 0.761$, $p = .518$, with a negligible effect size of $\omega^2 = 0.000$. Descriptive statistics indicated that mean GEI scores were relatively similar across groups: bachelor's degree ($M = 4.394$, $SD = 1.141$), doctoral degree ($M = 4.012$, $SD = 1.269$), master's degree ($M = 4.171$, $SD = 1.165$), and secondary school ($M = 4.186$, $SD = 1.141$).

Table 14. ANOVA - Education and GEI

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Education	3.119	3	1.040	0.761	0.518	0.000
Residuals	218.564	160	1.366			

Table 15. Descriptives - Education and GEI

Education	N	Mean	SD	SE	Coefficient of variation
Bachelor's degree	60	4.394	1.141	0.147	0.260
Doctoral degree	27	4.012	1.269	0.244	0.316
Master's degree	43	4.171	1.165	0.178	0.279
Secondary school	34	4.186	1.141	0.196	0.272

Table 16. Kruskal-Wallis Test - Education and GEI

Factor	Statistic	df	p
Education	1.412	3	0.703

To confirm these findings, post hoc comparisons were performed. Tukey's HSD test (Table 17) showed no significant differences between any of the education categories (all $p > .05$). Similarly, Dunnett's test (Table 18), which compared each group against the bachelor's degree group, did not reveal any statistically significant contrasts (all $p > .38$). Cohen's d values were all below 0.33, indicating small or negligible effect sizes.

Table 17. Standard HSD Post Hoc Comparisons - Education and GEI

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Bachelor's degree	Doctoral degree	0.382	0.271	160	1.411	0.327	0.495
	Master's degree	0.224	0.234	160	0.959	0.192	0.773
	Secondary school	0.208	0.251	160	0.830	0.178	0.840
Doctoral degree	Master's degree	−0.158	0.287	160	−0.551	−0.135	0.946
	Secondary school	−0.174	0.301	160	−0.577	−0.149	0.939
Master's degree	Secondary school	−0.016	0.268	160	−0.059	−0.013	1.000

Table 18. Dunnett Post Hoc Comparisons - Education and GEI

Comparison	Mean Difference	SE	t	$p_{dunnett}$
Doctoral degree - Bachelor's degree	−0.382	0.271	−1.411	0.380
Master's degree - Bachelor's degree	−0.224	0.234	−0.959	0.682
Secondary school - Bachelor's degree	−0.208	0.251	−0.830	0.767

The analysis did not show that individuals with different levels of formal education perceive differing degrees of control over cybersecurity outcomes. Perceived general controllability appears to be consistent across educational backgrounds in this sample.

4.6.3 Educational Differences in Cybersecurity Knowledge Scores

The analysis revealed a statistically significant difference in knowledge scores across education levels, $F(3, 160) = 3.440$, $p = .018$, with a small-to-moderate effect size ($\omega^2 = 0.043$). Descriptive statistics showed that participants with doctoral degrees had the highest mean knowledge score ($M = 17.778$, $SD = 8.308$), followed by those with master's degrees ($M = 16.186$, $SD = 7.142$), bachelor's degrees ($M = 15.167$, $SD = 7.665$), and secondary school education ($M = 11.882$, $SD = 7.446$).

Table 19. ANOVA - Education and Knowledge

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Education	595.471	3	198.490	3.440	0.018	0.043
Residuals	9233.041	160	57.707			

Table 20. Descriptives - Education and Knowledge

Education	N	Mean	SD	SE	Coefficient of variation
Bachelor's degree	60	15.167	7.665	0.990	0.505
Doctoral degree	27	17.778	8.308	1.599	0.467
Master's degree	43	16.186	7.142	1.089	0.441
Secondary school	34	11.882	7.446	1.277	0.627

Table 21. Kruskal-Wallis Test - Education and Knowledge

Factor	Statistic	df	p
Education	9.654	3	0.022

Post hoc analyses using Tukey's HSD test revealed a statistically significant difference between participants with doctoral degrees and those with secondary school education, $p = .016$, with a medium effect size ($d = 0.776$). Other pairwise comparisons did not reach statistical significance ($p > .05$), though the contrast between bachelor's degree and secondary school approached significance ($p = .187$, $d = 0.432$). Dunnett's test, comparing each group against the bachelor's degree group, found no significant differences, though the contrast with secondary education again approached significance ($p = .122$).

Table 22. Standard HSD Post Hoc Comparisons - Education and Knowledge

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Bachelor's degree	Doctoral degree	−2.611	1.760	160	−1.483	−0.344	0.450
	Master's degree	−1.019	1.518	160	−0.672	−0.134	0.908
	Secondary school	3.284	1.631	160	2.014	0.432	0.187
Doctoral degree	Master's degree	1.592	1.865	160	0.853	0.210	0.829
	Secondary school	5.895	1.958	160	3.011	0.776	0.016
Master's degree	Secondary school	4.304	1.743	160	2.469	0.567	0.069

Table 23. Dunnett Post Hoc Comparisons - Education and Knowledge

Comparison	Mean Difference	SE	t	$p_{dunnett}$
Doctoral degree - Bachelor's degree	2.611	1.760	1.483	0.339
Master's degree - Bachelor's degree	1.019	1.518	0.672	0.859
Secondary school - Bachelor's degree	−3.284	1.631	−2.014	0.122

The findings suggest that cybersecurity knowledge levels vary across educational backgrounds, particularly between those with secondary school education and those holding doctoral degrees. This supports the assumption that higher formal education may contribute to greater cybersecurity knowledge.

4.6.4 Educational Differences in Cybersecurity Behaviour

The results indicated that there were no statistically significant differences in behaviour scores between the education groups, $F(3, 160) = 1.022$, $p = .384$, with a negligible effect size ($\omega^2 = 4.098 \times 10^{-4}$). Descriptive statistics showed slight variations in mean behaviour scores: doctoral degree ($M = 22.704$, $SD = 4.921$), master's degree ($M = 22.442$, $SD = 5.483$), bachelor's degree ($M = 21.417$, $SD = 5.093$), and secondary school ($M = 20.824$, $SD = 4.914$).

Table 24. ANOVA - Education and Behaviour

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Education	80.894	3	26.965	1.022	0.384	4.098×10^{-4}
Residuals	4219.759	160	26.373			

Table 25. Descriptives - Education and Behaviour

Education	N	Mean	SD	SE	Coefficient of variation
Bachelor's degree	60	21.417	5.093	0.658	0.238
Doctoral degree	27	22.704	4.921	0.947	0.217
Master's degree	43	22.442	5.483	0.836	0.244
Secondary school	34	20.824	4.914	0.843	0.236

Table 26. Kruskal-Wallis Test - Education and Behaviour

Factor	Statistic	df	p
Education	3.902	3	0.272

Post hoc comparisons confirmed the non-significant ANOVA findings. Tukey's HSD test revealed that none of the pairwise group differences were statistically significant ($p > .05$), and effect sizes (Cohen's d) ranged from -0.251 to 0.366, indicating small or negligible effects. Dunnett's test, using the bachelor's degree group as the reference, also did not show any significant contrasts (all $p > .59$).

Table 27. Standard HSD Post Hoc Comparisons - Education and Behaviour

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Bachelor's degree	Doctoral degree	−1.287	1.190	160	−1.081	−0.251	0.701
	Master's degree	−1.025	1.026	160	−0.999	−0.200	0.750
	Secondary school	0.593	1.102	160	0.538	0.115	0.950
Doctoral degree	Master's degree	0.262	1.261	160	0.208	0.051	0.997
	Secondary school	1.880	1.324	160	1.420	0.366	0.489
Master's degree	Secondary school	1.618	1.179	160	1.373	0.315	0.518

Table 28. Dunnett Post Hoc Comparisons - Education and Behaviour

Comparison	Mean Difference	SE	t	$p_{dunnett}$
Doctoral degree - Bachelor's degree	1.287	1.190	1.081	0.597
Master's degree - Bachelor's degree	1.025	1.026	0.999	0.654
Secondary school - Bachelor's degree	−0.593	1.102	−0.538	0.920

While mean behaviour scores were slightly higher for participants with higher education, the differences were not statistically significant. This suggests that educational level alone may not be a strong predictor of cybersecurity behaviour.

4.7 Predicting Cybersecurity Behaviour from Knowledge, SEIS, and GEI

A linear regression was conducted to assess whether cybersecurity knowledge, self-efficacy (SEIS score), and general controllability (GEI score) predicted cybersecurity behaviour. In Model 0 (M_0), SEIS score and GEI score were entered. In Model 1 (M_1), knowledge score was added to evaluate its additional predictive value.

The results for M_0 indicated a significant model, $F(2, 161) = 7.588$, $p < .001$, with an $R^2 = 0.086$, meaning that SEIS and GEI together accounted for 8.6% of the variance in behaviour.

In M_1, the inclusion of knowledge score significantly improved the model, $F(3, 160) = 16.310$, $p < .001$, with an $R^2 = 0.234$, indicating that the model explained 23.4% of the variance in behaviour. The change in R^2 was significant, $\Delta R^2 = 0.148$, $F_{\text{change}}(1, 160) = 30.933$, $p < .001$, suggesting that knowledge contributes substantial explanatory power beyond SEIS and GEI.

Table 29. Model Summary - Predicting Behaviour

Model	R	R^2	Adjusted R^2	RMSE	R^2 Change	F Change	df1	df2	p
M_0	0.293	0.086	0.075	4.941	0.086	7.588	2	161	$< .001$
M_1	0.484	0.234	0.220	4.537	0.148	30.933	1	160	$< .001$

Table 30. ANOVA - Predicting Behaviour

Model		Sum of Squares	df	Mean Square	F	p
M_0	Regression	370.456	2	185.228	7.588	$< .001$
	Residual	3930.197	161	24.411		
	Total	4300.652	163			
M_1	Regression	1007.178	3	335.726	16.310	$< .001$
	Residual	3293.474	160	20.584		
	Total	4300.652	163			

Table 31. Coefficients - Predicting Behaviour

Model		Unstandardized	Standard Error	Standardized	t	p
M_0	(Intercept)	17.350	1.573		11.031	$< .001$
	SEIS SCORE	1.091	0.309	0.293	3.526	$< .001$
	GEI SCORE	0.007	0.366	0.002	0.020	0.984
M_1	(Intercept)	16.446	1.453		11.316	$< .001$
	SEIS SCORE	0.170	0.329	0.046	0.517	0.606
	GEI SCORE	0.013	0.336	0.003	0.037	0.970
	Total score (knowledge, out of 34)	0.302	0.054	0.457	5.562	$< .001$

These findings indicate that although self-efficacy initially appears to predict behaviour, its effect diminishes when knowledge is included. The final model supports the conclusion that actual cybersecurity knowledge is a stronger and more consistent predictor of behavioural practices than self-perceived confidence or perceived controllability.

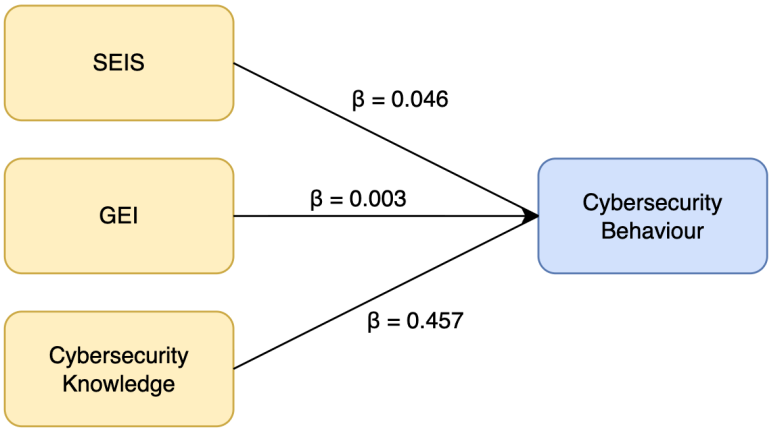

Figure 2. *Predicting Cybersecurity Behaviour from Knowledge, Self-Efficacy, and General Controllability*

4.8 Mediation Analysis: The Role of Knowledge in the Relationship Between SEIS, GEI, and Behaviour

A mediation analysis was conducted to examine whether cybersecurity knowledge mediates the relationships between self-efficacy (SEIS score) and general controllability (GEI score) as predictors, and cybersecurity behaviour as the outcome. The maximum likelihood estimator was used. The proposed mediation model included SEIS score and GEI score as exogenous variables, knowledge as the mediator, and behaviour as the dependent variable. The direct path from SEIS score to behaviour was not statistically significant, with an unstandardised estimate of 0.170, $SE = 0.325$, $z = 0.524$, $p = .601$, 95% CI $[-0.466, 0.806]$. Similarly, the direct effect of GEI score on behaviour was also non-significant, 0.013, $SE = 0.332$, $z = 0.038$, $p = .970$, 95% CI $[-0.638, 0.663]$.

Table 32. Direct effects

			Estimate	Std. error	z-value	p	95% Confidence Interval
SEIS SCORE	→	Total score (behaviour, out of 36)	0.170	0.325	0.524	0.601	−0.466 0.806
GEI SCORE	→	Total score (behaviour, out of 36)	0.013	0.332	0.038	0.970	−0.638 0.663

The indirect effect of SEIS score on behaviour via knowledge was statistically significant, with an estimate of 0.921, $SE = 0.205$, $z = 4.495$, $p < .001$, 95% CI $[0.519, 1.322]$. This indicates a meaningful mediation effect, whereby greater self-efficacy increases knowledge, which in turn increases safe behavioural practices. In contrast, the indirect effect of GEI score on behaviour via knowledge was not significant, -0.005, $SE = 0.146$, $z = -0.036$, $p = .971$, 95% CI $[-0.291, 0.281]$.

Table 33. Indirect effects

					Estimate	Std. error	z-value	p	95% Confidence Interval	
SEIS SCORE	→	Total score (knowledge, out of 34)	→	Total score (behaviour, out of 36)	0.921	0.205	4.495	< .001	0.519	1.322
GEI SCORE	→	Total score (knowledge, out of 34)	→	Total score (behaviour, out of 36)	−0.005	0.146	−0.036	0.971	−0.291	0.281

The total effect of SEIS score on behaviour was statistically significant, 1.091, $SE = 0.306$, $z = 3.559$, $p < .001$, suggesting a substantial combined direct and indirect influence. However, the total effect of GEI score on behaviour was not significant, 0.007, $SE = 0.362$, $z = 0.020$, $p = .984$.

Table 34. Total effects

			Estimate	Std. error	z-value	p	95% Confidence Interval
SEIS SCORE	→	Total score (behaviour, out of 36)	1.091	0.306	3.559	< .001	0.490 1.691
GEI SCORE	→	Total score (behaviour, out of 36)	0.007	0.362	0.020	0.984	−0.703 0.718

The mediating variable, knowledge, significantly predicted behaviour ($\beta = 0.302$, $p < .001$) and was significantly predicted by SEIS score ($\beta = 3.045$, $p < .001$). GEI score, however, was not a significant predictor of either behaviour or knowledge.

Table 35. Path coefficients

			Estimate	Std. error	z-value	p	95% Confidence Interval
Total score (knowledge, out of 34)	→	Total score (behaviour, out of 36)	0.302	0.054	5.631	< .001	0.197 0.408
SEIS SCORE	→	Total score (behaviour, out of 36)	0.170	0.325	0.524	0.601	−0.466 0.806
GEI SCORE	→	Total score (behaviour, out of 36)	0.013	0.332	0.038	0.970	−0.638 0.663
SEIS SCORE	→	Total score (knowledge, out of 34)	3.045	0.408	7.463	< .001	2.245 3.844
GEI SCORE	→	Total score (knowledge, out of 34)	−0.018	0.482	−0.036	0.971	−0.963 0.928

Table 36. R-Squared

	R^2
Total score (behaviour, out of 36)	0.234
Total score (knowledge, out of 34)	0.291

The model accounted for 23.4% of the variance in cybersecurity behaviour and 29.1% of the variance in knowledge, as shown in Table 36.

The mediation model shows that cybersecurity knowledge fully mediates the relationship between self-efficacy and behaviour. Self-efficacy alone does not directly influence behaviour but rather enhances knowledge, which then leads to safer behavioural outcomes. Conversely, GEI does not significantly influence knowledge or behaviour, either directly or indirectly.

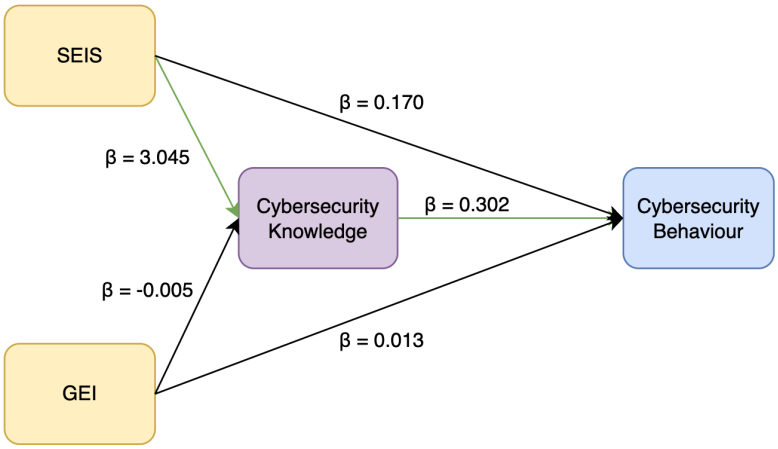

Figure 3. *Mediation Analysis: The Role of Knowledge in the Relationship Between SEIS, GEI, and Behaviour*

4.9 Predicting Cybersecurity Knowledge from SEIS and GEI

A linear regression analysis was performed to examine whether self-efficacy (SEIS score) and general controllability (GEI score) significantly predict cybersecurity knowledge. Both SEIS and GEI were entered simultaneously into the model.

The overall model was statistically significant, $F(2, 161) = 33.079$, $p < .001$, and explained approximately 29.1% of the variance in cybersecurity knowledge ($R^2 = 0.291$), as shown in Table 37.

Analysis of the individual predictors revealed that only SEIS score was a significant positive predictor of cybersecurity knowledge, with an unstandardised coefficient of 3.045 ($SE = 0.412$), $t = 7.395$, $p < .001$, and a standardised beta coefficient of 0.541. GEI score was not a significant predictor ($\beta = -0.003$, $t = -0.036$, $p = .971$).

Table 37. Model Summary - SEIS, GEI and Knowledge

Model	R	R^2	Adjusted R^2	RMSE
M_0	0.000	0.000	0.000	7.765
M_1	0.540	0.291	0.282	6.578

Table 38. ANOVA - SEIS, GEI and Knowledge

Model		Sum of Squares	df	Mean Square	F	p
M_1	Regression	2862.506	2	1431.253	33.079	< .001
	Residual	6966.006	161	43.267		
	Total	9828.512	163			

Table 39. Coefficients - SEIS, GEI and Knowledge

Model		Unstandardized	Standard Error	Standardized	t	p
M_0	(Intercept)	15.183	0.606		25.040	< .001
M_1	(Intercept)	2.989	2.094		1.427	0.155
	SEIS SCORE	3.045	0.412	0.541	7.395	< .001
	GEI SCORE	−0.018	0.487	−0.003	−0.036	0.971

The regression results demonstrate that higher self-efficacy is strongly associated with greater cybersecurity knowledge, while perceived general controllability does not significantly contribute to explaining knowledge levels.

4.10 Differences in Cybersecurity Knowledge and Behaviour by Perceived Expertise

ANOVA was conducted to test whether cybersecurity knowledge and behaviour scores differed significantly based on self-perceived expertise in cybersecurity (novice, intermediate, advanced, expert). The dependent variables were the total knowledge and behaviour scores, and ω^2 was reported as a measure of effect size.

4.10.1 Differences in Cybersecurity Knowledge by Perceived Expertise

The ANOVA was statistically significant, $F(3, 160) = 17.222$, $p < .001$, indicating that perceived expertise groups differed in terms of cybersecurity knowledge. The effect size was substantial, $\omega^2 = 0.229$, meaning that 22.9% of the variance in knowledge scores could be explained by perceived expertise. Descriptive statistics revealed a clear upward trend in mean knowledge scores with increasing perceived expertise: novice ($M = 11.255$, $SD = 6.755$), intermediate ($M = 12.622$, $SD = 6.125$), advanced ($M = 17.576$, $SD = 7.211$), and expert ($M = 23.857$, $SD = 6.792$). This pattern was also visualised in a bar plot (see Figure **??**).

Table 40. ANOVA - Perceived Expertise and Knowledge

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Perceived expertise	2399.038	3	799.679	17.222	< .001	0.229
Residuals	7429.474	160	46.434			

Table 41. Descriptives - Perceived Expertise and Knowledge

Perceived expertise	N	Mean	SD	SE	Coefficient of variation
Novice	47	11.255	6.755	0.985	0.600
Intermediate	37	12.622	6.125	1.007	0.485
Advanced	66	17.576	7.211	0.888	0.410
Expert	14	23.857	6.792	1.815	0.285

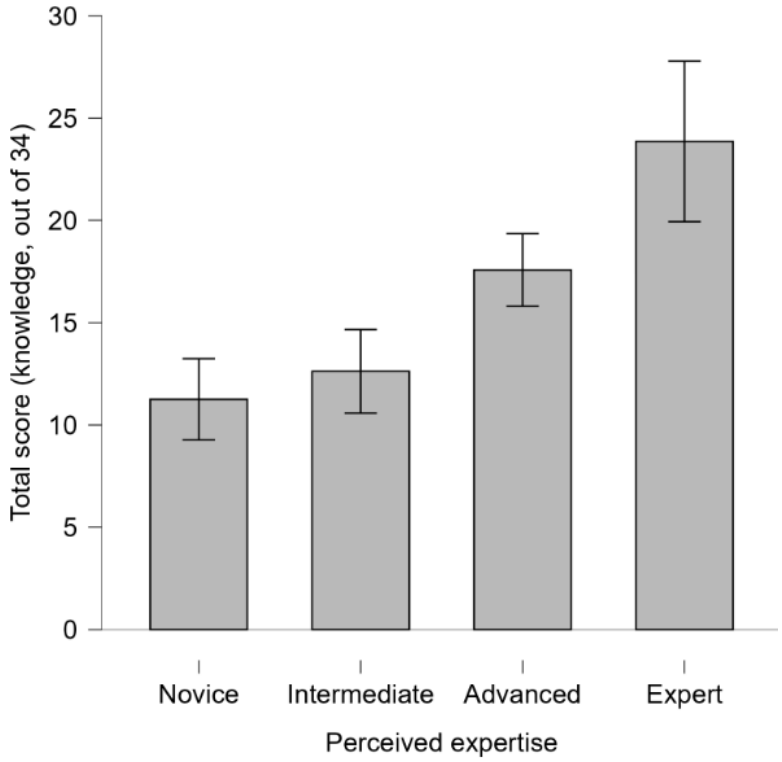

Figure 4. *Perceived Expertise and Knowledge Bar Plot*

Post hoc comparisons using Tukey's HSD test showed significant differences between most group pairs. Experts had significantly higher knowledge scores than all other groups: novice ($p < .001$, $d = -1.849$), intermediate ($p < .001$, $d = -1.649$), and advanced ($p = .011$, $d = -0.922$). Advanced participants also scored significantly higher than novices ($p < .001$, $d = -0.928$) and intermediates ($p = .003$, $d = -0.727$). However, the difference between novice and intermediate groups was not statistically significant ($p = .798$).

Table 42. Post Hoc Comparisons - Perceived expertise

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Novice	Intermediate	−1.366	1.498	160	−0.912	−0.201	0.798
	Advanced	−6.320	1.301	160	−4.860	−0.928	< .001
	Expert	−12.602	2.075	160	−6.074	−1.849	< .001
Intermediate	Advanced	−4.954	1.399	160	−3.540	−0.727	0.003
	Expert	−11.236	2.138	160	−5.255	−1.649	< .001
Advanced	Expert	−6.281	2.005	160	−3.133	−0.922	0.011

These results suggest that individuals' self-assessed cybersecurity expertise aligns strongly with their actual knowledge. Perceived expertise appears to be a meaningful and accurate indicator of cybersecurity knowledge.

4.10.2 Differences in Cybersecurity Behaviour by Perceived Expertise

The ANOVA result did not reach statistical significance, $F(3, 160) = 2.215$, $p = .088$, although the effect size was small but non-negligible, $\omega^2 = 0.022$. Descriptive statistics indicated a slight upward trend in behaviour scores with higher levels of perceived expertise: novice ($M = 20.723$, $SD = 5.064$), intermediate ($M = 20.865$, $SD = 5.094$), advanced ($M = 22.727$, $SD = 4.610$), and expert ($M = 23.214$, $SD = 6.985$), as also illustrated in Figure 5.

Table 43. ANOVA - Perceived Expertise and Behaviour

Cases	Sum of Squares	df	Mean Square	F	p	ω^2
Perceived expertise	171.476	3	57.159	2.215	0.088	0.022
Residuals	4129.177	160	25.807			

Table 44. Descriptives - Perceived Expertise and Behaviour

Perceived expertise	N	Mean	SD	SE	Coefficient of variation
Novice	47	20.723	5.064	0.739	0.244
Intermediate	37	20.865	5.094	0.838	0.244
Advanced	66	22.727	4.610	0.567	0.203
Expert	14	23.214	6.985	1.867	0.301

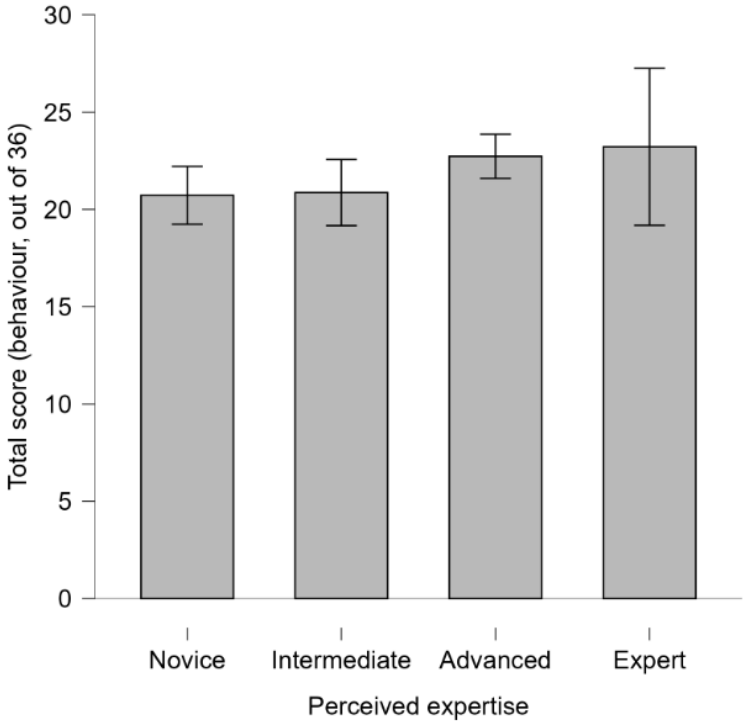

Figure 5. *Perceived Expertise and Behaviour Bar Plot*

Post hoc comparisons using Tukey's HSD test showed that none of the pairwise comparisons between perceived expertise groups reached statistical significance ($p > .05$ in all cases). Cohen's d values for effect size ranged from -0.096 to -0.490, suggesting small effect sizes across the group comparisons.

Table 45. Post Hoc Comparisons - Perceived Expertise and Behaviour

		Mean Difference	SE	df	t	Cohen's d	p_{tukey}
Novice	Intermediate	-0.141	1.117	160	-0.127	-0.028	0.999
	Advanced	-2.004	0.970	160	-2.067	-0.394	0.169
	Expert	-2.491	1.547	160	-1.610	-0.490	0.376
Intermediate	Advanced	-1.862	1.043	160	-1.785	-0.367	0.284
	Expert	-2.349	1.594	160	-1.474	-0.462	0.456
Advanced	Expert	-0.487	1.495	160	-0.326	-0.096	0.988

While the behavioural data showed a modest increasing trend in cybersecurity practices with higher perceived expertise, this difference was not statistically significant. Therefore, perceived expertise does not appear to be a robust predictor of actual cybersecurity behaviour in this sample.

4.11 Multivariate Differences in Knowledge and Behaviour by Perceived Expertise

A MANOVA was conducted to assess whether levels of perceived cybersecurity expertise (novice, intermediate, advanced, expert) had a statistically significant multivariate effect on participants' combined cybersecurity knowledge and behaviour scores. Pillai's Trace was used as the multivariate test statistic. Despite the data's non-normality, MANOVA was conducted because it offers a robust method for evaluating differences across multiple dependent variables (knowledge and behaviour) simultaneously, and is relatively robust to moderate violations of normality in large samples.

The MANOVA revealed a statistically significant multivariate effect of perceived expertise on the combined dependent variables, $V = 0.253$, $F(6, 320) = 7.722$, $p < .001$, suggesting that self-rated expertise meaningfully influences at least one of the outcome variables. Additionally, ANOVAs indicated that perceived expertise significantly predicted knowledge scores, $F(3, 160) = 17.222$, $p < .001$, but did not significantly predict behaviour scores, $F(3, 160) = 2.215$, $p = .088$. These findings replicate and confirm the earlier independent ANOVA results: while perceived expertise is strongly associated with actual knowledge, its influence on cybersecurity behaviour is minimal and statistically non-significant.

Table 46. MANOVA: Pillai Test

Cases	df	Approx. F	Trace$_{Pillai}$	Num df	Den df	p
(Intercept)	1	1504.572	0.950	2	159.000	$<$ .001
Perceived expertise	3	7.722	0.253	6	320.000	$<$ .001
Residuals	160					

Table 47. ANOVA: Perceived expertise - knowledge and behaviour

Cases	Sum of Squares	df	Mean Square	F	p
(Intercept)	37805.488	1	37805.488	814.173	$<$ .001
Perceived expertise	2399.038	3	799.679	17.222	$<$ .001
Residuals	7429.474	160	46.434		

Perceived expertise appears to be a valid predictor of cybersecurity knowledge but does not cybersecurity behaviour.

Table 48. ANOVA: Perceived expertise - knowledge and behaviour

Cases	Sum of Squares	df	Mean Square	F	p
(Intercept)	77756.348	1	77756.348	3012.953	$< .001$
Perceived expertise	171.476	3	57.159	2.215	0.088
Residuals	4129.177	160	25.807		

4.12 Linear Regression: Predicting Cybersecurity Behaviour with Knowledge, SEIS, and GEI (Factoring Education, Gender, and Perceived Expertise)

4.12.1 Factoring Education

A hierarchical linear regression analysis was conducted to assess the combined predictive effect of self-efficacy (SEIS), general expertise (GEI), cybersecurity knowledge, and education level on cybersecurity behaviour scores. In the initial model (M_0), SEIS and GEI were entered. In the extended model (M_1), total knowledge score and education level were added.

Model M_0, which included only SEIS and GEI, was statistically significant, $F(2, 161) = 7.588$, $p < .001$, and explained 8.6% of the variance in behaviour scores ($R^2 = 0.086$). The addition of total knowledge score and education in model M_1 significantly improved the model, $F(6, 157) = 8.158$, $p < .001$, raising the explained variance to 23.8% ($R^2 = 0.238$).
Examining the individual predictors in model M_1, only cybersecurity knowledge significantly predicted behaviour ($\beta = 0.453$, $t = 5.374$, $p < .001$). SEIS ($\beta = 0.049$, $t = 0.542$, $p = .589$), GEI ($\beta = 0.008$, $t = 0.107$, $p = .915$), and all education categories (vs. bachelor's degree) were non-significant predictors ($p > .426$ in all cases).

Table 49. Model Summary: Factoring Education

Model	R	R^2	Adjusted R^2	RMSE
M_0	0.293	0.086	0.075	4.941
M_1	0.488	0.238	0.209	4.570

Table 50. ANOVA: Factoring Education

Model		Sum of Squares	df	Mean Square	F	p
M_0	Regression	370.456	2	185.228	7.588	< .001
	Residual	3930.197	161	24.411		
	Total	4300.652	163			
M_1	Regression	1022.139	6	170.356	8.158	< .001
	Residual	3278.514	157	20.882		
	Total	4300.652	163			

Table 51. Coefficients: Factoring Education

Model		Unstandardized	Standard Error	Standardized	t	p
M_0	(Intercept)	17.350	1.573		11.031	< .001
	SEIS SCORE	1.091	0.309	0.293	3.526	< .001
	GEI SCORE	0.007	0.366	0.002	0.020	0.984
M_1	(Intercept)	15.957	1.597		9.995	< .001
	SEIS SCORE	0.181	0.334	0.049	0.542	0.589
	GEI SCORE	0.037	0.342	0.008	0.107	0.915
	Total score (knowledge, out of 34)	0.300	0.056	0.453	5.374	< .001
	Education (Doctoral degree)	0.512	1.077		0.476	0.635
	Education (Master's degree)	0.732	0.918		0.798	0.426
	Education (Secondary school)	0.522	1.000		0.522	0.602

These results suggest that among the variables tested, cybersecurity knowledge is the strongest and only significant predictor of secure behaviour, while self-efficacy, general expertise, and education level do not meaningfully contribute to the prediction when knowledge is included in the model.

4.12.2 Factoring Gender

Another hierarchical linear regression was conducted to assess whether gender contributed to the prediction of cybersecurity behaviour beyond self-efficacy (SEIS), general expertise (GEI), and cybersecurity knowledge. In the first model (M_0), SEIS and GEI were entered. In the second model (M_1), knowledge score and gender were added.

Model M_0 was statistically significant, $F(2, 161) = 7.588$, $p < .001$, accounting for 8.6% of the variance in behaviour scores ($R^2 = 0.086$). The inclusion of knowledge and gender in M_1 improved the model, $F(4, 159) = 13.837$, $p < .001$, increasing the explained variance to 25.8% ($R^2 = 0.258$).
In the final model M_1, cybersecurity knowledge remained the strongest predictor of behaviour ($\beta = 0.480$, $t = 5.869$, $p < .001$), while gender also significantly contributed to the model. Specifically, identifying as male (with female coded as the reference group)

was associated with lower behaviour scores ($\beta = -0.173$, $t = -2.269$, $p = .025$). SEIS ($p = .168$) and GEI ($p = .799$) were not significant predictors.

Table 52. Model Summary: Factoring Gender

Model	R	R^2	Adjusted R^2	RMSE
M_0	0.293	0.086	0.075	4.941
M_1	0.508	0.258	0.240	4.479

Table 53. ANOVA: Factoring Gender

Model		Sum of Squares	df	Mean Square	F	p
M_0	Regression	370.456	2	185.228	7.588	$< .001$
	Residual	3930.197	161	24.411		
	Total	4300.652	163			
M_1	Regression	1110.510	4	277.627	13.837	$< .001$
	Residual	3190.143	159	20.064		
	Total	4300.652	163			

Table 54. Coefficients: Factoring Gender

Model		Unstandardized	Standard Error	Standardized	t	p
M_0	(Intercept)	17.350	1.573		11.031	$< .001$
	SEIS SCORE	1.091	0.309	0.293	3.526	$< .001$
	GEI SCORE	0.007	0.366	0.002	0.020	0.984
M_1	(Intercept)	16.016	1.447		11.066	$< .001$
	SEIS SCORE	0.491	0.354	0.132	1.386	0.168
	GEI SCORE	−0.085	0.334	−0.019	−0.255	0.799
	Total score (knowledge, out of 34)	0.317	0.054	0.480	5.869	$< .001$
	Gender (Male)	−1.945	0.857		−2.269	0.025

These results indicate that, beyond knowledge, gender plays a small but statistically significant role in predicting cybersecurity behaviour, with males reporting slightly lower behaviour scores than females, all else being equal. While self-efficacy (SEIS) was a significant predictor in the initial model, its effect decreased when knowledge and gender were accounted for. This suggests that females may exhibit more secure behaviour despite lower SEIS scores.

4.12.3 Factoring Perceived Expertise

A hierarchical linear regression was conducted to examine whether perceived expertise significantly predicts cybersecurity behaviour beyond self-efficacy (SEIS), general exper-

tise (GEI), and cybersecurity knowledge. In the initial model (M_0), SEIS and GEI were entered. The second model (M_1) added knowledge and perceived expertise.

Model M_0 was significant, $F(2, 161) = 7.588$, $p < .001$, with an explained variance of $R^2 = 0.086$. The inclusion of knowledge and perceived expertise in M_1 significantly improved the model, $F(6, 157) = 8.641$, $p < .001$, with $R^2 = 0.248$ and an adjusted $R^2 = 0.220$.

In M_1, cybersecurity knowledge was a significant positive predictor of behaviour ($\beta = 0.479$, $t = 5.690$, $p < .001$). SEIS ($p = .239$) and GEI ($p = .900$) were not significant. None of the perceived expertise categories (Intermediate: $p = .675$; Advanced: $p = .533$; Expert: $p = .097$) significantly predicted behaviour compared to the reference group (Novice), although the Expert category approached significance and had a relatively large negative unstandardised coefficient ($B = -2.988$).

Table 55. Model Summary: Factoring Perceived Expertise

Model	R	R^2	Adjusted R^2	RMSE
M_0	0.293	0.086	0.075	4.941
M_1	0.498	0.248	0.220	4.538

Table 56. ANOVA: Factoring Perceived Expertise

Model		Sum of Squares	df	Mean Square	F	p
M_0	Regression	370.456	2	185.228	7.588	< .001
	Residual	3930.197	161	24.411		
	Total	4300.652	163			
M_1	Regression	1067.643	6	177.940	8.641	< .001
	Residual	3233.010	157	20.592		
	Total	4300.652	163			

Table 57. Coefficients: Factoring Perceived Expertise

Model		Unstandardized	Standard Error	Standardized	t	p
M_0	(Intercept)	17.350	1.573		11.031	< .001
	SEIS SCORE	1.091	0.309	0.293	3.526	< .001
	GEI SCORE	0.007	0.366	0.002	0.020	0.984
M_1	(Intercept)	15.553	1.635		9.514	< .001
	SEIS SCORE	0.455	0.385	0.122	1.181	0.239
	GEI SCORE	0.043	0.340	0.010	0.126	0.900
	Total score (knowledge, out of 34)	0.317	0.056	0.479	5.690	< .001
	Perceived expertise (Intermediate)	−0.422	1.006		−0.420	0.675
	Perceived expertise (Advanced)	−0.632	1.011		−0.625	0.533
	Perceived expertise (Expert)	−2.988	1.787		−1.672	0.097

These findings suggest that cybersecurity knowledge remains the most robust predictor of behavioural scores, whereas self-perceived expertise does not independently contribute significantly once knowledge is factored.

5. Discussion and Interpretation

5.1 Chapter Overview

This chapter interprets and contextualises the results presented in Chapter 4 by linking them to existing literature and the study's research questions. The discussion compares the results to either or both international and Slovenian literature where possible. The chapter provides a critical and evidence-based interpretation of cybersecurity knowledge, behaviour, and self-perceptions among Slovenians.

When interpreting the results presented in this chapter, it is important to acknowledge a key limitation inherent to correlational analysis. Specifically, correlation coefficients only indicate the strength and direction of association between variables but do not imply causality. A statistically significant correlation does not necessarily mean that one variable causes changes in the other. Therefore, findings based on correlation should be understood as indicative of association rather than evidence of direct causal influence. This caution is especially relevant when drawing conclusions about behavioural outcomes and psychological constructs.

5.2 Discussion and Interpretation of Findings

The analysis revealed no significant correlation between GEI and reported cybersecurity behaviour, indicating that participants' **general perceived control over threats does not necessarily translate into secure behaviour**. This finding suggests a cognitive-behavioural gap: although individuals may feel cyber risks can be managed in general, this confidence does not manifest in consistent or effective security practices. This distinction is critical for cybersecurity training and awareness efforts, as it implies that perceived controllability alone is insufficient for behavioural change.

The gender-based analysis (Table 7) revealed that **male participants reported significantly higher levels of self-efficacy and showed better cybersecurity knowledge**. However, these differences did not extend to actual reported cybersecurity behaviour. **No statistically significant gender disparity was observed in behaviour**. This suggests that while men in the sample may feel more confident and possess more theoretical knowledge, this does not necessarily translate into safer or more consistent security practices. Such a discrepancy may reflect broader psychological or sociocultural influences. Particularly

gender differences in confidence and self-efficacy. This finding aligns with the findings of other studies on gender differences in self-efficacy. For example, a study on Age and Gender Differences in ICT Cybersecurity Behaviour found that males reported higher levels of self-efficacy compared to females [55]. Additionally, despite the observed differences in self-efficacy, gender was not a significant predictor of actual cybersecurity behaviour.

The linear regression analysis examining SEIS, GEI, and cybersecurity knowledge revealed that SEIS was significantly associated with higher knowledge scores. In contrast, GEI showed no meaningful relationship with knowledge. These findings suggest that **self-efficacy plays an important cognitive role in motivating individuals to obtain and retain cybersecurity knowledge**. Confidence in one's abilities may encourage more active engagement with cybersecurity-related content and a greater willingness to learn it.

The multivariate analysis in Section 4.11 confirmed the earlier ANOVA results, showing that **perceived cybersecurity expertise is strongly associated with actual knowledge but has minimal and statistically non-significant influence on reported cybersecurity behaviour**. This pattern indicates that while individuals who consider themselves more knowledgeable about cybersecurity tend to perform better on knowledge assessment, but this perception does not reliably translate into more secure practices. The dissociation between cognitive belief and behavioural execution highlights a challenge in the cybersecurity: the knowledge–behaviour gap. Despite being aware of risks and protective strategies, individuals may still fail to implement them consistently, possibly due to habits, convenience, or perceived effort. Studies in the literature review consistently showed that individuals often overestimate their cybersecurity competence, which leads to risky online practices despite awareness of best practices [40, 28]. This overconfidence, combined with the habitual ignorance of privacy policies and consent notices, further highlights the contrast between perceived and actual online security behaviour [39].

An examination of cybersecurity self-efficacy (SEIS) across different education levels (Tables 9, 10, and 11) revealed a descriptive trend suggesting that participants with higher formal education tended to report slightly greater self-efficacy. However, these differences did not reach statistical significance. The study provides **no conclusive evidence that cybersecurity self-efficacy is systematically influenced by level of formal education**. This finding aligns with previous research by Sámson and Tick [42], who found that self-initiated education, rather than formal institutional training, was a stronger predictor of secure cybersecurity behaviour, and that demographic variables (including education level) had minimal impact on awareness.

Complementing the self-efficacy findings, the analysis also examined differences in cy-

bersecurity knowledge across educational levels. In this case, statistically significant differences were observed, with higher education levels generally associated with better performance on the knowledge test. However, this interpretation can be deceiving. The actual scores were notably low. Even PhD level participants scored only around 50% on average. This suggests that while formal education may contribute modestly to improved cybersecurity knowledge, it does not mean users have even the foundational understanding of key concepts or best practices.

As shown in Table 31, only SEIS was a significant predictor of cybersecurity behaviour in this model, while GEI was not. In the full model, knowledge emerged as the strongest predictor, while SEIS became non-significant, and GEI remained non-significant. This suggests that while confidence in one's cybersecurity abilities (SEIS) may initially appear influential, its predictive power is insignificant when actual knowledge is accounted for. In practical terms, this indicates that (rather than perceived capability or general feelings of control) **knowledge is the most robust determinant of secure behaviour**.

The mediation analysis further reinforced the role of cybersecurity knowledge in shaping behavioural outcomes. While both knowledge and SEIS were initially associated with behaviour, the effect of SEIS was significantly reduced when knowledge was introduced as a mediator, suggesting that much of SEIS's apparent influence is through its connection to actual knowledge. In other words, **individuals who feel confident in their cybersecurity abilities are more likely to engage in secure behaviour primarily because they tend to possess greater knowledge, not only due to their confidence**. The literature review similarly emphasised that knowledge alone is often insufficient to drive behavioural change [40]. This analysis suggests it remains a fundamental prerequisite for meaningful improvement in practice. For example, Cravens and Resch found that while CS students only marginally outperformed non-CS peers on cybersecurity knowledge tests, their password hygiene was significantly better. This indicates that even modest gains in knowledge can result in better behavioural outcomes. This suggests the idea that although knowledge is not the only factor, it is a necessary foundation for effective cybersecurity practices.

5.3 Answering Research Questions

Based on the statistical analysis of the data collected from 164 Slovenian participants, this section provides definitive answers to the research questions. It also highlights key similarities and differences between the findings from this study and those reported in the literature review.

1. **MRQ: What is the current state of cybersecurity knowledge and behaviour among Slovenians?**
   The analysis confirmed that the general state of cybersecurity knowledge among Slovenians is alarmingly low, even among highly educated participants. Although those with higher education scored better, even PhD-level participants performed poorly on average. Behavioural results revealed that self-reported practices were also lacking, with significant gaps between what participants knew and how they behaved. Many continued to report risky practices such as weak password use, neglecting software updates, or inconsistent use of multi-factor authentication.
   Comparison to literature review: These results reinforce the literature review's conclusion that Slovenians are overconfident in their cybersecurity competence and frequently engage in unsafe practices despite moderate awareness [14, 26, 48]. Specifically, the thesis builds on findings such as those by Šolic et al. [28], who identified a privacy paradox through behavioural experiments, and confirms that over 20% of participants in this study revealed a password or reused credentials despite knowing the risks. Unlike the previous literature, which often focused on students or urban populations, this study provides representative, population-level confirmation of these behavioural contradictions and cognitive biases.
2. **SRQ1: What is the level of self-efficacy for information security among Slovenians?**
   The results indicated that men, on average, scored significantly higher on the SEIS scale compared to women. However, overall self-efficacy did not consistently predict cybersecurity behaviour when knowledge was controlled for. Education level had no significant effect on SEIS. These findings suggest that while many participants report confidence in their abilities, this confidence does not necessarily result in safer behaviour.
   Comparison to literature review: The literature suggested that self-efficacy may be overestimated and that it plays a complex role in shaping behaviour [14, 26, 23, 38]. This study confirms those assumptions and extends them by using the SEIS scale to show that even high self-efficacy scores did not translate into safer practices. In particular, findings complement the work by Mihelič et al. [23], who noted that confidence alone among older adults failed to predict technology adoption unless knowledge and perceived usefulness were also high. Similarly, this study shows that knowledge mediates the relationship between self-efficacy and behaviour, which was not empirically demonstrated in prior Slovenian literature.
3. **SRQ2: What is the level of cybersecurity knowledge among Slovenians?**
   Cybersecurity knowledge was generally low across the sample. While participants with higher education showed slightly better results, the average knowledge scores were far below optimal levels. Regression analysis found that SEIS predicted

knowledge level, but GEI did not.

Comparison to literature review: These findings match the literature's picture of fragmented and insufficient knowledge among Slovenian users [26, 27, 19]. For example, Klein et al. [19] found that only students with prior IT training demonstrated meaningful cybersecurity knowledge. This thesis confirms and expands on that by showing, with a larger and more demographically varied sample, that such knowledge gaps are not restricted to students but are widespread across the general population. Furthermore, unlike prior studies which used simple awareness items, this thesis used graded knowledge questions, which offers more generalisable results.

4. **SRQ3: What are the actual cybersecurity behaviours of Slovenians?**
   The analysis revealed that self-reported cybersecurity behaviour was only weakly associated with self-efficacy or general controllability. Instead, knowledge emerged as the strongest predictor of secure behaviour. The gender analysis showed no significant behavioural differences despite men scoring higher on both SEIS and knowledge, which further suggests that confidence and knowledge do not guarantee secure practices.

   Comparison to literature review: The results support previous findings on the knowledge–behaviour gap and the influence of psychological factors such as overconfidence [28, 39, 40]. In particular, this study aligns with Cravens and Resch [40], who noted that even computer science students with better knowledge did not always demonstrate secure password behaviour. The main contribution of this study is its demonstration (via regression and mediation analysis) that only actual knowledge (not perceived competence or control) significantly predicts behaviour. This provides a more definitive answer than prior Slovenian studies, which often speculated about this gap without statistically isolating the role of each variable.

5.4 Study Limitations

Despite the strengths of this study, some limitations must be acknowledged to contextualise the findings. A central challenge was the lack of existing empirical research in the Slovenian context, which limited the ability to directly compare this study's findings with prior national benchmarks. Most comparative references had to be drawn from international literature findings, which correlate to different cultural, educational, and infrastructural frameworks. Similarly, publicly available Slovenian cybersecurity data is sparse or non-existent, and even Slovenia's national cybersecurity strategy [5] lacks empirical grounding, offering little in terms of population-level statistics or concrete measures. Methodologically, the cross-sectional design of this thesis captures a state in current time and cannot track changes in knowledge, behaviour or attitudes over time. A longitudinal study is needed to display differences over time. Additionally, although the

sample was demographically diverse, it may not be fully representative of all segments of the Slovenian population, especially those less digitally active or with limited access to online surveys. Lastly, the reliance on self-reported behaviour introduces the possibility of social desirability bias, where participants may overstate their cybersecurity competence or underreport risky practices. These limitations underscore the need for more sustained, context-specific, and longitudinal research on cybersecurity in Slovenia. It also underscores the need for more Slovenian research in general.

6. Conclusions and Recommendations

6.1 Conclusions

This study set out to investigate the state of cybersecurity knowledge and behaviour among Slovenians, with particular attention to the roles of self-efficacy (SEIS), general controllability (GEI), and knowledge. The findings highlight several critical gaps in both public understanding and behavioural security practices.

Firstly, the observed educational differences in SEIS demonstrate that higher education does not necessarily equate to stronger cybersecurity self-efficacy. Even doctoral-level participants exhibited surprisingly low knowledge scores. This challenges assumptions that formal education alone correlates with higher security knowledge. This highlights the need for targeted interventions across all education levels, and not only among those perceived as digitally underinformed.

Secondly, the regression analyses confirm that SEIS significantly predicts cybersecurity knowledge. This suggests that building an individual's belief in their capability to understand cybersecurity might help motivate and push users to learn more about cybersecurity. Consequently, training programmes should not only spread technical content but also aim to encourage a sense of control and confidence in participants.

However, when predicting actual cybersecurity behaviour, knowledge emerged as the strongest predictor, outweighing self-belief. Individuals with higher knowledge scores consistently demonstrated more secure digital habits. This aligns with the mediation analysis, which showed that knowledge mediates the effect of SEIS and GEI on behaviour. While boosting confidence remains important, it should serve a complementary role to factual knowledge.

Notably, the study reveals a deficiency in cybersecurity knowledge across all educational categories, underscoring the deficiency of current education and awareness measures in Slovenia. Given that even highly educated individuals perform poorly, cybersecurity must be introduced early, starting from primary education and continuing as a compulsory topic through secondary, undergraduate, and postgraduate levels.

Finally, the correlation between confidence and knowledge should be interpreted cautiously.

Correlation does not imply causation, and an overemphasis on boosting confidence without substantive skill-building could risk creating a false sense of security.

6.2 Actionable Recommendations

Based on the above conclusions and aligned with gaps identified in national and EU-level strategic documents, the following actionable recommendations are proposed:

1. **Integrate cybersecurity education across all levels of formal education**, from primary school through to doctoral programmes. Introduce it not as an optional module, but as a mandatory introductory subject tailored to each educational stage. This directly addresses the Slovenian Cybersecurity Strategy's recognised weakness (the absence of cybersecurity in school curricul) [5] and operationalises ENISA's call for lifelong cybersecurity education across member states [8].
2. **Develop national awareness campaigns with dual focus**: deliver practical, skill-based knowledge while simultaneously supporting confidence-building through real-life examples and achievable scenarios. Campaigns should not rely on abstract warnings but demonstrate step-by-step how users can act securely. This recommendation strengthens the vague "awareness-raising" goal in the Slovenian strategy [5] and responds to the strategy's lack of measurable campaign effectiveness. It also aligns with ENISA's guidance on culturally relevant outreach [8].
3. **Establish digital security workshops**, particularly aimed at adults outside formal education. These workshops should emphasise hands-on learning, address common misconceptions, and be delivered in accessible formats for all age groups. This operationalises the strategy's general ambition to involve the wider population, particularly digitally vulnerable groups such as older adults [5], and aligns with the inclusive goals of the upcoming ZInfV-1 implementation under NIS2 [16].
4. **Update teacher training programmes and professional development** to include cybersecurity basics, ensuring that educators themselves are equipped to pass on knowledge and demonstrate safe behaviour. The 2016 strategy acknowledges the need to "strengthen human capital" [5] but does not provide mechanisms. This fills that gap and reflects ENISA's emphasis on education-sector engagement [8].
5. **Support media literacy initiatives** that explicitly include cybersecurity competence as a key component. This should go beyond general digital literacy to incorporate threat recognition, behavioural cues, and response strategies. While the Slovenian strategy mentions "raising digital literacy," [5] it does not distinguish media literacy from cybersecurity. This recommendation clarifies and bridges that strategic ambiguity.
6. **Incorporate confidence-building techniques in training** (e.g. simulated phishing

tests with feedback, personal data protection checklists, or gamified modules), but ensure that they are always rooted in accurate and verifiable knowledge. This responds to the overconfidence and behaviour–knowledge gap discussed both in this thesis and the literature, and offers concrete implementation ideas absent in the national strategy.

7. **Collaborate with tech companies and ISPs** to create simplified, jargon-free guides and nudges during digital onboarding processes (e.g. setting up a router, creating accounts), targeting user involvement. This meets the strategy's stated goal of involving the private sector [5] but proposes practical actions that involve the users, which is currently missing from the strategic framework.
8. **Launch a national certification** for personal cybersecurity competence, enabling individuals to demonstrate basic digital hygiene knowledge in both professional and everyday contexts. Such a certification could support workforce upskilling, in line with Slovenia's digital transformation goals [5], and complements the EU's broader efforts under the NIS2 directive to build security competence across sectors [16].

6.3 Future Work

While this study provides important insight into the cybersecurity knowledge, behaviour, and self-efficacy of Slovenians, it also reveals the need for further research that could deepen understanding and support the development in this field.

1. **Longitudinal Studies of Behavioural Change.** The present research is cross-sectional and captures behaviour and perception at a single point in time. A longitudinal approach would be necessary to evaluate sustained behavioural change and the long-term effectiveness of educational or awareness interventions. For instance, tracking the same group of participants before and after attending a cybersecurity training programme, with follow-up assessments at three, six, and twelve months, could reveal how knowledge retention and behavioural improvements evolve or regress over time.
2. **Experimental Designs with Control Groups.** Future studies could implement controlled experiments in educational or workplace settings. For example, randomly assigning participants to receive either a traditional awareness campaign, an interactive hands-on workshop, or no intervention (control), and comparing knowledge and behavioural outcomes post-intervention. Such a design would allow for a robust evaluation of different teaching methods and content delivery strategies.
3. **Early-Age Curriculum Trials.** Given the finding that even highly educated individuals scored poorly on cybersecurity knowledge, programmes could be designed and tested in Slovenian primary and secondary schools. These should include pre/post-

testing, assessment of engagement, and teacher feedback. Ideally, they would test different levels of content complexity to determine the optimal starting age and instructional style for cybersecurity education.

4. **Self-Efficacy Interventions and Measurement.** Since SEIS was found to predict knowledge, it would be valuable to design and test brief psychological interventions aimed at increasing cybersecurity self-efficacy. For example, using task-specific feedback, one could measure whether changes in SEIS directly enhance learning and behavioural outcomes. These studies would clarify whether self-efficacy is a modifiable variable with causal influence, not just correlational.
5. **Cybersecurity Behaviour under Stress and Time Pressure.** Building on literature suggesting that real-world decisions often occur under pressure [37], future work could explore how stress affects Slovenian users' adherence to security practices. Simulated tasks (e.g. inbox sorting under time limits) combined with eye-tracking or behavioural logs could assess whether users ignore security cues when under cognitive load.
6. **Representative Population-Level Surveys.** Although this study drew from diverse educational and demographic backgrounds, future work should aim for even more representative sampling across Slovenia. It would also be interesting to test whether living in rural or urban places has a measurable effect on cybersecurity knowledge and behaviour.

These directions aim to move the field from description to intervention, ensuring that future studies are both empirically rigorous and policy-relevant. Overall, they encourage more empirical research in this field. By combining experimental, longitudinal, and applied designs, future research can better inform educational reform, national strategy, and personal resilience towards growing digital threats.

References

[1] Adam Beautement, M Angela Sasse, and Mike Wonham. "The compliance budget: Managing security behaviour in organisations". In: *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 2008, pp. 47–58. DOI: 10.1145/1595676.1595684.

[2] M Angela Sasse, Sacha Brostoff, and Dirk Weirich. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security". In: *BT Technology Journal* 19.3 (2001), pp. 122–131. DOI: 10.1023/A:1011902718709.

[3] Ponemon Institute. *The Cybersecurity in the Remote Work Era: A Global Risk Report*. https://www.ponemon.org/library/the-cybersecurity-in-the-remote-work-era-a-global-risk-report. Accessed: 2025-04-22. 2020.

[4] SI-CERT. *Kibernetska varnost 2024 v številkah*. 2024. URL: https://www.cert.si/kibernetska-varnost-2024-v-stevilkah/ (visited on 03/02/2025).

[5] Government of the Republic of Slovenia. *Cyber Security Strategy of the Republic of Slovenia*. Available at: https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf. 2016.

[6] Government of the Republic of Slovenia. *National Security*. Accessed: 2025-04-28. 2023. URL: https://www.gov.si/en/policies/defence-civil-protection-and-public-order/national-security/.

[7] Damjan Štrucl. *National Cybersecurity Organisation: Slovenia*. Tech. rep. NATO Cooperative Cyber Defence Centre of Excellence, Aug. 2021. URL: https://ccdcoe.org/uploads/2021/08/Slovenia_country_report_final_for_publication_August_2021.pdf.

[8] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. 2023.

[9] European Commission. *2030 Digital Compass: The European Way for the Digital Decade*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118. 2021.

[10] Kathryn Parsons et al. “Cultural influences on cybersecurity behaviours: A new model of security culture”. In: *ACM Transactions on Computer-Human Interaction* 24.3 (2017), pp. 1–23. DOI: 10.1145/3058552.

[11] Albert Bandura. *Self-efficacy: The exercise of control*. W. H. Freeman, 1997.

[12] Moti Zwilling et al. “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study”. In: *Journal of Computer Information Systems* (2020). DOI: 10.1080/08874417.2020.1712269.

[13] PRISMA Group. *PRISMA Statement: Preferred Reporting Items for Systematic Reviews and Meta-Analyses*. https://www.prisma-statement.org/. Accessed: 2025-02-20. PRISMA Executive, Monash University, 2020. URL: https://www.prisma-statement.org/.

[14] Igor Bernik. “Cybersecurity of Slovenia and its Citizens”. In: *2nd National Conference on Local Safety and Security: Safety and Security in Local Communities*. Ed. by Gorazd Meško, Katja Eman, and Urška Pirnat. Maribor, Slovenia: University of Maribor Press, 2016, pp. 101–108. ISBN: 978-961-286-001-1. DOI: 10.18690/978-961-286-001-1.12. URL: http://press.um.si.

[15] Republic of Slovenia. *Kazenski zakonik (KZ-1)*. sl. https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050. Official Gazette of the Republic of Slovenia, No. 55/08, with subsequent amendments. 2008. URL: https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050.

[16] European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555. OJ L 333, 27.12.2022, pp. 80–152. Dec. 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

[17] Eversheds Sutherland. *Slovenia - EU NIS2 Directive*. 2025. URL: https://ezine.eversheds-sutherland.com/eu-nis2-directive/slovenia.

[18] European Commission. *Commission calls on 23 Member States to fully transpose NIS2 Directive*. 2024. URL: https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive.

[19] Galit Klein, Moti Zwilling, and Dušan Lesjak. “A Comparative Study in Israel and Slovenia Regarding the Awareness, Knowledge, and Behavior Regarding Cyber Security”. In: *Cybersecurity Risk Management in Cyber-Physical Systems*. Ed. by D. P. Kumar, S. El-Hadary, and P. M. El-Kafrawy. IGI Global, 2021, pp. 97–121. DOI: 10.4018/978-1-7998-8586-6.ch005. URL: https://www.igi-global.com/chapter/a-comparative-study-in-israel-and-slovenia-regarding-the-awareness-knowledge-and-behavior-regarding-cyber-security/288690.

[20] Maja Dakić et al. *Cross-cultural validation and psychometric testing of the Slovenian version of the Croatian Behavioral-Cognitive Internet Security Questionnaire (BCISQ)*. https://repozitorij.unios.hr/islandora/object/foozos:1777. Accessed: 28 April 2025. 2022.

[21] Igor Bernik, Kaja Prislan, and Anže Mihelič. “Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia”. In: *Sustainability* 14.21 (2022). ISSN: 2071-1050. URL: https://www.mdpi.com/2071-1050/14/21/14487.

[22] Simon Vrhovec and Blaž Markelj. “We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers”. In: *PLOS ONE* 19 (Oct. 2024), pp. 1–27. DOI: 10.1371/journal.pone.0312266. URL: https://doi.org/10.1371/journal.pone.0312266.

[23] Kaja Prislan Mihelič et al. “Perceived Threat of Cyber Attacks and its Role in the Adoption of Tablet Computers by Older Adults”. In: *Central European Conference on Information and Intelligent Systems*. Faculty of Organization and Informatics Varazdin. 2023, pp. 49–56.

[24] Ilija Ilievski and Igor Bernik. “Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje”. In: *2. Nacionalna konferenca o varnosti v lokalnih skupnostih: Varnost v lokalnih skupnostih*. Ed. by Gorazd Meško, Katja Eman, and Urška Pirnat. Maribor, Slovenia: University of Maribor Press, 2016, pp. 75–84. ISBN: 978-961-286-001-1. DOI: 10.18690/978-961-286-001-1.10. URL: https://press.um.si/index.php/ump/catalog/view/174/154/246-1.

[25] The Slovenia Times. “Police Commissioner Calls for Powers to Fight Cyber Crime”. In: *The Slovenia Times* (Jan. 2020). Accessed: 2025-03-30. URL: https://sloveniatimes.com/15586/police-commissioner-calls-for-powers-to-fight-cyber-crime.

[26] Blaž Markelj and Sabina Zgaga. “Comprehension of cyber threats and their consequences in Slovenia”. In: *Computer Law Security Review* 32.3 (2016), pp. 513–525. ISSN: 2212-473X. DOI: https://doi.org/10.1016/j.clsr.2016.01.006. URL: https://www.sciencedirect.com/science/article/pii/S0267364916300206.

[27] Borka Jerman Blazic, Primož Cigoj, and Andrej Jerman Blažič. “Web-Service Security and The Digital Skills of Users: An Exploratory Study of Countries in Europe”. In: *J. Internet Services Inf. Secur* 13.3 (2023), pp. 41–57.

[28] Krešimir Šolić, Robert Idlbek, and Tena Velki. “An Empirical Study on Differences Between Self-Assessed and Measured Real Risk in Online Behaviour”. In: *International Journal of Electrical and Computer Engineering Systems* 15.3 (2024). Accessed: 2025-03-28, pp. 297–304. ISSN: 1847-7003. URL: https://doi.org/10.32985/ijeces.15.3.8.

[29] A. Sangwan. “Human Factors in Cybersecurity Awareness”. In: *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*. 2024, pp. 1–7. DOI: 10.1109/ISCS61804.2024.10581139.

[30] N. Y.-R. Douha et al. “Smart home cybersecurity awareness and behavioral incentives”. In: *Information Computer Security* 31.5 (2023), pp. 545–575. DOI: 10.1108/ICS-03-2023-0032.

[31] J. Taylor-Jackson et al. “Incorporating psychology into cyber security education: A pedagogical approach”. In: *Financial Cryptography and Data Security*. Ed. by M. Bernhard et al. Cham: Springer, 2020, pp. 207–217. DOI: 10.1007/978-3-030-54455-3_15.

[32] T. Mashiane and E. Kritzinger. “Cybersecurity Behaviour: A Conceptual Taxonomy”. In: *Information Security Theory and Practice. WISTP 2018*. Ed. by O. Blazy and C. Yeun. Vol. 11469. Lecture Notes in Computer Science. Cham: Springer, 2019. DOI: 10.1007/978-3-030-20074-9_11.

[33] D. Köhler, W. Pünter, and C. Meinel. “How vulnerable is the average population? Advocating for cybersecurity awareness education in people’s private lives”. In: *Proc. CHI Conf. Human Factors Comput. Syst. (CHI ’23)*. Hamburg, Germany, 2023. DOI: 10.13140/RG.2.2.24781.65760.

[34] S. Sütterlin et al. “Individual deep fake recognition skills are affected by viewer’s political orientation, agreement with content and device used”. In: *Augmented Cognition. HCII 2023*. Ed. by D. D. Schmorrow and C. M. Fidopiastis. Cham: Springer, 2023, pp. 269–284. DOI: 10.1007/978-3-031-35017-7_18.

[35] M. Owen, S. V. Flowerday, and K. van der Schyff. “Optimism bias in susceptibility to phishing attacks: An empirical study”. In: *Information Computer Security* (2024). DOI: 10.1108/ICS-02-2023-0023.

[36] Daniel Sturman et al. “The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection”. In: *Applied Ergonomics* 119 (2024), p. 104309. ISSN: 0003-6870. DOI: https://doi.org/10.1016/j.apergo.2024.104309. URL: https://www.sciencedirect.com/science/article/pii/S0003687024000863.

[37] N. H. Chowdhury, M. T. P. Adam, and G. Skinner. “The impact of time pressure on cybersecurity behaviour: a systematic literature review”. In: *Behaviour & Information Technology* 38.12 (2019), pp. 1290–1308. DOI: 10.1080/0144929X.2019.1583769.

[38] M. Dupuis et al. “The use and non-use of cybersecurity tools among consumers: Do they want help?” In: *Proceedings of the 20th Annual Conference on Information Technology Education (SIGITE ’19)*. Tacoma, WA, USA, 2019, pp. 81–86. DOI: 10.1145/3349266.3351419.

[39] J. A. Obar and A. Oeldorf-Hirsch. “The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services”. In: *Information, Communication & Society* 23.1 (2020), pp. 128–147. DOI: 10.1080/1369118X.2018.1486870.

[40] Dalton Cravens and Cheryl Resch. “Comparison of Password Hygiene for Computer Science and Non-Computer Science Undergraduates”. In: *Proceedings of the 24th Annual Conference on Information Technology Education*. 2023, pp. 112–117.

[41] S. Kankane, C. DiRusso, and C. Buckley. “Can we nudge users toward better password management? An initial study”. In: *CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI ’18)*. Montreal, QC, Canada, Apr. 2018, pp. 1–6. DOI: 10.1145/3170427.3188689.

[42] N. Sámson and A. Tick. “Digital Defense: Investigating Human Aspects of Cybersecurity”. In: *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. Timisoara, Romania, 2024, pp. 000525–000532. DOI: 10.1109/SACI60582.2024.10619840.

[43] D. Snyman and H. Kruger. “The role of information deserts in information security awareness and behaviour”. In: *Proceedings of the 8th International Conference on Information Systems Security and Privacy*. 2022, pp. 613–620.

[44] Hyeun-Suk Rhee, Cheongtag Kim, and Young Ryu. “Self-efficacy in information security: Its influence on end users’ information security practice behavior”. In: *Computers Security* 28 (Nov. 2009), pp. 816–826. DOI: 10.1016/j.cose.2009.05.008.

[45] Xin (Robert) Luo et al. “Social engineering: The neglected human factor for information security management”. In: *Information Resources Management Journal* 24.3 (2011), pp. 1–8. DOI: 10.4018/irmj.2011070101.

[46] Norhafizah Che Zainal, Mohd Hazwan Mohd Puad, and Nor Fazlida Mohd Sani. “Moderating Effect of Self-Efficacy in the Relationship Between Knowledge, Attitude and Environment Behavior of Cybersecurity Awareness”. In: *Asian Social Science* 18.1 (2022), pp. 55–64. DOI: 10.5539/ass.v18n1p55. URL: https://doi.org/10.5539/ass.v18n1p55.

[47] Michael Workman. “Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security”. In: *Journal of the American Society for Information Science and Technology* 59.4 (2008), pp. 662–674. DOI: 10.1002/asi.20779.

[48] Simon Vrhovec et al. “Cybersecurity competence of older adult users of mobile devices”. In: *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*. 2024, pp. 221–223.

[49] Heinrich-Heine-Universität Düsseldorf. *G*Power [Computer software]*. https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower. Accessed: 2025-04-01.

[50] Google LLC. *Google Forms [Computer software]*. https://www.google.com/forms/about/. Accessed: 2025-04-01. 2024.

[51] Legalweb.io. *Google Forms (Workspace) and the GDPR*. Accessed: 2025-05-12. n.d. URL: https://legalweb.io/en/gdpr/embeddings_googleforms_workspace/.

[52] Measured Collective. *Is Google Forms GDPR Compliant?* Accessed: 2025-05-12. n.d. URL: https://measuredcollective.com/is-google-forms-gdpr-compliant/.

[53] JASP Team. *JASP (Version 0.19.3) [Computer software]*. 2025. URL: https://jasp-stats.org/.

[54] Mark A. Goss-Sampson. *Statistical Analysis in JASP 2024: A Guide for Students*. Version 0.18.3. 2024. URL: https://jasp-stats.org/wp-content/uploads/2024/03/Statistical-Analysis-in-JASP-2024.pdf.

[55] Dawn Branley-Bell et al. “Exploring Age and Gender Differences in ICT Cybersecurity Behaviour”. In: *Human Behavior and Emerging Technologies* 2022 (2022). Article ID 2693080, pp. 1–10. DOI: 10.1155/2022/2693080. URL: https://doi.org/10.1155/2022/2693080.

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

I Luka Kerin

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Cybersecurity knowledge and behaviour among Slovenians", supervised by Ricardo Gregorio Lugo
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.2025

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

Appendix 2 – SEIS and GEI Questions

SEIS

1. I feel confident handling virus infected files.
2. I feel confident getting rid of spyware.
3. I feel confident understanding terms/words relating to information security.
4. I feel confident learning the method to protect my information and
5. information system.
6. I feel confident managing files in my computer.
7. I feel confident setting the Web browser to different security levels.
8. I feel confident using different programs to protect my information and
9. information system.
10. I feel confident learning advanced skills to protect my information and
11. information system.
12. I feel confident getting help for problems related to my information security.
13. I feel confident using the user's guide when help is needed to protect my information and information system.
14. I feel confident updating security patches to the operating system.

GEI

1. In general, threats to information security are controllable.
2. In general, technology is advanced enough to prevent information security threats.
3. In general, there exist means to control information security threats.