FACULTY OF SCIENCE & TECHNOLOGY

Understanding student engagement with online platforms for cybersecurity training

By

Pooja Pooja

A thesis submitted in fulfilment of the requirements for the degree of Master by Research

Bournemouth University

Copyright statement:

Dissertation Declaration

I understand that if Bournemouth University decide to keep a copy of my dissertation as a reference, then it will be kept normally for 3 academic years. I know that after the given retention time my dissertation will be destroyed.

Confidentiality

The personal details of the participants have been anonymised, with the exception of those participants who gave permission for them to be published if they belong to it. I have checked this Dissertation and certify that no information of a commercial and confidential type or of any personal nature other than usually found in the public domain has been included in it except with the necessary permission. Any information which refers to certain person's faith or politics, health and/or anthropological data, criminal past or intimate relations with others has been removed or anonymized to protect participant privacy.

Copyright

The copyright for this dissertation remains with me.

Requests for Information

I agree that this dissertation may be made available as the result of a request for information under the Freedom of Information Act.

Signed: POOJA .

Name: POOJA

Date:12/05/2026

Programme: Master's by research, Faculty of Science and Technology

Original Work Declaration

This dissertation and the project that it is based on are my work, except where stated, by university regulations.

Signed: POOJA .

Name: POOJA

Date: 12/5/2026

Acknowledgments

I would like to thank Dr. Jane Henriksen-Bulmer, Nicholas Mavengere and Vasilis Katos for their supervision, support and constructive criticism during this research. I also would like to acknowledge those at Bournemouth University and the Faculty of Science and Technology that helped create this study. In addition, I would like to sincerely thank the employees and students who helped to enable the secondary analysis from the pilot cybersecurity training program. Lastly, I would like to express my gratitude to my parents, for their patience, encouragement, and continued support throughout the writing of this thesis.

Abstract

The increasing utilization of digital learning spaces in higher learning has also highlighted the issue of effective IT education within digital learning spaces among the students. The adoption of IT tools for cybersecurity awareness programmes has become very popular, but it is dependent on the technological and behavioural aspects. Online utilisation of online platforms in cybersecurity training presents both challenges and opportunities for higher education students, and in this dissertation the authors look at the barriers as well as the benefits and behavioral factors that impact outcomes related to security. In the present instance, the cases relied on the quantitative approach to case study analysis coupled with secondary data analysis for establishing relationships between problematic Internet use, impulsiveness, and security behaviour intentions, and cyber performance. The findings highlight that behavioural traits prove to be crucial factors when it comes to students' engagement in cybersecurity training and their ability to translate awareness into secure practices and behaviour. User behaviour and engagement pose limitations on the performance of online platforms, while allowing a more scalable, accessible and uniform delivery of training. The research points to the need to consider the human factor in addition to technical in creating cybersecurity education programmes. This study contributes to the research literature on cybersecurity education by demonstrating the need for behaviour-oriented computer security training courses in the university. Practical implications are provided to the universities, teachers and institutional security departments to enhance student awareness and practices pertaining to cyber security. In terms of future research, further research into the degree of behavioural study and the impact of the online cybersecurity training interventions over time is needed.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Introduction to the Study

The ISC2 Cybersecurity Workforce Study found that many professionals enter cybersecurity field from non-technical backgrounds, highlighting the value of interdisciplinary skills (ISC2, 2022). By receiving cybersecurity training, all students gain a foundational awareness that prepares them to use technology responsibly and safely in both their personal and professional lives. It also encourages critical thinking and risk awareness, which are valuable skills in any field (Center for Internet Security [CIS], 2021). Thus, cybersecurity training should not be limited to IT-related fields, students from any discipline will use and rely on digital systems in their future careers. For example, a business student may need to understand how to handle customer data securely, or a healthcare student must learn to protect patient records. Therefore, introducing cybersecurity training earlier, while they are studying would not only enhance their skills and knowledge, it would enhance their employability. To facilitate this, Bournemouth University (BU) collaborated with their staff cybersecurity training provider, KnowBe4, to introduce cybersecurity training to the student population at BU.

1.2 Background of Cybersecurity in Higher Education

The need for robust cybersecurity measures has never been more pressing as the digital landscape continues to evolve. With increasing reliance on online systems for academic, administrative, and personal purposes, universities, particularly in the United Kingdom, have become prime targets for cyberattacks (Jisc, 2020). This growing threat has highlighted the critical importance of cybersecurity training. According to the UK government's National Cyber Security Centre (NCSC), the number of cyberattacks is rising, and the skills gap in cybersecurity is widening. This shift is driven by the recognition that cybersecurity is everyone's responsibility. As the National Cyber Strategy, UK cyber ecosystem has invested in up-skilling the people and strengthening partnerships between academia, government and industry, acting as one of the central pillar to its National Cyber Strategy (HM Government, 2022). Staff at all levels in an organisation are potential targets for cyberattacks, especially in terms of social engineering tactics like phishing. Many businesses and universities have introduced basic cybersecurity training for their staff, focusing on best practices for data security, recognising phishing attempts, password management, and maintaining secure access to networks and systems (Omolola 2022).

1.3 Emergence of Online Platforms and Universities for Cybersecurity Training

The role of universities is crucial in educating and preparing future cybersecurity professionals. However, the role of online training platforms is equally important for this research. Adopting an online cybersecurity training programme to deliver cybersecurity training to students brings affordability, cost-effectiveness and real-time training opportunities. Passive learning methods such as one-time webinars, reading materials, or quizzes may provide the necessary knowledge to students from non-IT disciplines, but they do not always translate into real-world application or behavioural changes (Li et al. 2024). Conversely, students in IT-related programs are more likely to be exposed to more comprehensive training, making them better prepared for professional cybersecurity roles (Gichoya and Reilly, 2018).

Thus, Students should be actively involved in security and digital forensics tasks, including identifying vulnerabilities, configuring firewalls, performing penetration testing, and applying encryption techniques to help prevent and mitigate potential cyberattacks. For the students who are from a non-IT background, they should be more focused on awareness and being updated regarding the technological upgrades and shifts to keep their devices secure from cyber threats and make sure that the security settings, such as firewalls and software updates, are properly maintained.

Online platforms can cater to the diverse learning needs of both students and staff, offering a range of training formats such as modules, webinars, and simulations. However, the implementation of online cybersecurity comes with its challenges, such as engagement, maintaining high-quality content, security of online platforms and addressing the varying levels of cybersecurity knowledge among students, that may affect the effectiveness of the training (Alasmary and Alhaidari, 2020).

1.4 Factors affecting training effectiveness

The effectiveness of this cybersecurity training is to train technical and non-technical students to become more vigilant about cybersecurity threats and adopt security-conscious behaviours to reduce cyber risks, unlike technical training. Engagement refers to the level of attention, curiosity, interest, and motivation students show during learning. High engagement is crucial in cybersecurity education, as it promotes deeper understanding and retention of security practices (Knowles et al., 2014). Methods such as gamification, simulations, and real-world scenarios have been shown to enhance engagement by making learning more interactive and relevant (Tschakert and Ngamsuriyaroj, 2019).

Predispositions significantly influence how students engage with and benefit from cybersecurity training. Motivation and self-efficacy play a central role; students who believe in their ability to understand cybersecurity concepts are more likely to participate actively and persist through challenges. Risk perception also affects engagement: when students view cyber threats as personally relevant, they are more attentive and more likely to adopt secure behaviors (Ng, Kankanhalli, and Xu, 2009). Additionally, prior experience and familiarity with technology or cybersecurity concepts can ease the learning process, making the content more accessible and reducing cognitive load. In contrast, students with limited background may feel overwhelmed, leading to lower engagement and retention (Alshaikh, 2020). Finally, cognitive styles and learning preferences further shape training effectiveness.

1.5 Rationale for Cybersecurity Training Among Non-Technical Students

A report by the UK government (2023) has shown that in 2022, 85% of higher educational institutions experienced cyberattacks and data breaches. These challenges necessitate a proactive approach to cybersecurity that the rapid expansion of digital technologies in higher education has brought about significant benefits, including increased accessibility, collaboration, and efficiency. However, it has also led to a growing vulnerability to cybersecurity threats. Universities, as institutions, are responsible for safeguarding sensitive academic, financial, and personal data, and, as a result, universities have increasingly become targets for cybercriminals. In the UK, cyberattacks on universities have been reported to escalate, with incidents ranging from ransomware attacks to data breaches (NCSC, 2020) Thus, this study will argue that universities should consider not just staff and how they handle data, but also the student population, through comprehensive training programs for students, who are integral to the protection of institutional systems and data.

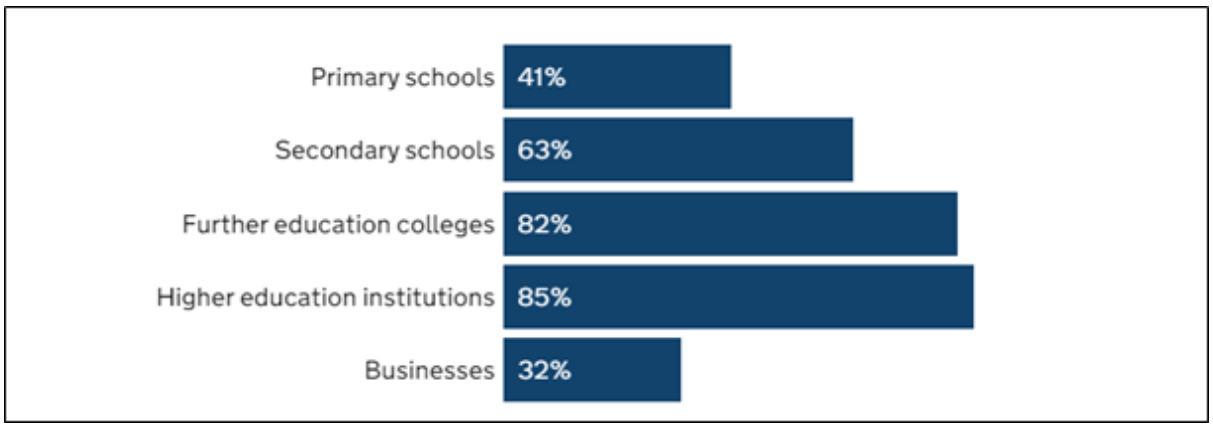


Figure 1: Percentage of organisations that have identified breaches or attacks in the last 12 months (Anderson, 2020)

Historically, universities have relied on face-to-face training sessions to enhance cybersecurity awareness. However, such traditional methods have limitations in terms of accessibility, scalability, and the ability to accommodate large and diverse populations (Anderson, 2020). Online platforms offer a promising alternative by providing flexible, cost-effective, and widely accessible training. These platforms can reach a wide audience at scale, delivering training content in various formats, including interactive modules, webinars, and simulations, which cater to diverse learning styles (Sharma and Rathi, 2021). This makes online cybersecurity education a particularly viable solution for UK universities that need to address the growing need for cybersecurity awareness without overburdening them. BU has adopted this approach, offering cybersecurity training to staff through a third-party company that offers online staff training.

1.6 Problem Statement

This research will look at what the opportunities and barriers are to delivering online cybersecurity training programs to students. The study will seek to understand the effectiveness, benefits, and opportunities of delivering cybersecurity training to students, to address the existing gaps in cybersecurity training among the student population, which is essential for building resilience among businesses and national security. The study focuses on engagement levels, behavioural traits and whether behavioural traits affect levels of engagement.

Understanding student engagement with online platforms for cybersecurity training, and analyse cybersecurity training provision and levels of engagement specifically within educational programs, thereby seeking to provide insights into how universities can better prepare their students to protect themselves and the institution from cyber threats providing both theoretical knowledge and practical skills to meet the growing demands of the cybersecurity field.

Effective training programs result in higher performance on exams, quizzes, and other assessments, demonstrating that students have understood the theoretical material (Ho et al. 2024). Effectiveness refers to how well a cybersecurity training program meets its educational goals and objectives, particularly in enhancing students' knowledge, skills, and competencies. Effective cybersecurity training ensures that students not only grasp theoretical concepts but

also gain practical, real-world skills to handle security challenges. Effective training programs result in higher performance on exams, quizzes, and other assessments, demonstrating that students have understood the theoretical material (Ho et al. 2024). Students should be able to recognise potential cybersecurity threats, understand the gravity of the threat and mitigate it as soon as any threat arises. Post training, both IT and non-IT students and staff of the cybersecurity training should respond to the cybersecurity incidents appropriately and timely manner. Their goal should be to reduce the risk of data breaches and other cybersecurity-related issues.

1.6.1 KnowBe4 Pilot Study

KnowBe4, Bournemouth University's (BU) cybersecurity training provider for staff, approached BU academics about the idea of delivering similar cybersecurity training to students to that provided for staff, and a pilot training programme was put together to establish how effective such training might be.

The programme of training saw BU deliver 7 training modules to all students (a cohort of approximately 18k students) covering: internet security, security awareness, secure online behaviour, security culture, phishing, online scamming, and acceptable use of technology. The training was delivered via the university's VLE and participation was entirely voluntary. As part of this pilot study, raw data was collected from BU students over a period of approximately one year. Before undertaking the training modules, a pre-test questionnaire was used to assess students' behavioural traits around security, internet use, and levels of impulsiveness. The data from this programme will be used in this study to inform the findings and recommendations of this study.

1.7 Research Questions

The research will ask the following questions:

RQ1: How do individual behavioural traits affect student engagement and completion of online cybersecurity training?

RQ2: What effect does study subject area/matter have on engagement levels and completion rates of cybersecurity training across different cohorts?

1.8 Research Aim and Objectives

1.8.1 Research Aim

This research aim is to understand student engagement with online platforms for cybersecurity training, and whether personality traits such as problematic internet use (PIU) (Demetrovics et al., 2016), security behaviour intentions (SEBIS) (Egelman and Peer, 2015), and the Abbreviated Impulsiveness Scale (ABIS) (Coutlee et al., 2014) influence how students engage with learning materials.

Research Objectives

To achieve this aim, the following objectives have been discussed and set so that the sub-questions can be answered:

1. To investigate the impact of problematic internet use (PIU) on students' intentions to engage in secure online behaviours.
2. To examine the relationship between abbreviated impulsiveness and students' security behaviour intentions in an online context.
3. To determine the role of demographic factors (e.g., gender, department, course) in moderating the relationships among internet use, impulsiveness, security intentions, and training performance.
4. To explore how individual traits (e.g., impulsiveness and internet use behaviour) and intentions contribute to successful engagement with online cybersecurity training.

1.8.3 Hypothesis

To support these questions three hypothesis (H) are put forward:

- H1: Students who have good security behavioural traits (SEBIS) are less likely to have Problematic Internet use (PIU) traits also?
- H2: Students who have higher levels of impulsivity are negatively associated with secure cybersecurity behaviours.
- H3: Cyber performance of students in different cohorts is significantly impacted by the Security Behaviours Intentions (SEBIS), Abbreviated Impulsiveness (AI) and Problematic Internet Use (PIU).

1.9 Significance of the Study

The study has a significant impact in the study of cybersecurity education, since it goes beyond the current studies on the topic of cybersecurity awareness education in higher education institutions, to incorporate views of behavioural and engagement based approaches to the matter. According to Armas and Taherdoost (2025), a cybersecurity-aware culture in universities can only be developed through a change in the approach involving technical controls to more organised educational interventions that impact individual behaviour.

According to Al-Sherideh et al. (2023), cybersecurity carried out in the scope of e-learning has varying success in interaction with users and context design, which can cause a situation requiring informed decision-making by institutions. This research, therefore, assists universities to make training efforts to resonate with the behavioural patterns of students.

The research is also informative to the policy makers and institution security groups as it gives an understanding of how student awareness will minimise the human factor related to cyber risks. Wiechetek and Mędrek (2022) also postulated that the non-technical students constitute a very important but, at the same time, undervalued population of cybersecurity measures, and, therefore, the inclusiveness of the training policies is relevant. Moreover, instructors providing cybersecurity education online can be favourable to comprehend pedagogical implications of platform-based cybersecurity education. Finally, the study aids enhanced digital safety and employability of students both in the long term and by building the much-needed skills in so-called cyber hygiene, and this study is nevertheless highly consistent with the UK higher education priorities in cybersecurity.

1.10 Structure of the Dissertation

The thesis is structured into eight chapters. Chapter 1 introduces the topic of online cybersecurity training among students and presents the research questions, aim, objectives, rationale and scope. Chapter 2 reviews literature on cybersecurity training, digital literacy, online delivery models and behavioural traits. Chapter 3 outlines the methodology. Chapter 4 presents the analysis of the data and discusses the hypotheses. Chapter 5 develops the design implications for student-focused online cybersecurity training. Chapter 6 evaluates the benefits and challenges of the online training approach. Chapter 7 provides recommendations for practice, policy and future research. Chapter 8 concludes the thesis.

2 LITERATURE REVIEW

2.1 Introduction

The shift to online education has significantly impacted how students engage with and perform in cybersecurity training modules. As cybersecurity becomes an increasingly critical area of expertise, universities have adopted online platforms to deliver specialised learning experiences that are flexible and scalable. Research on student performance in online cybersecurity courses highlights the importance of interactive learning tools, such as virtual labs, simulations, and real-time feedback, which support students in applying theoretical knowledge to practical situations. These tools are shown to improve student engagement and skill retention (Anderson, 2020; Hall, 2021). Online education has also revolutionised the teaching, assessment as well as professional training in higher education institutions due to its booming growth in the higher training institution. Online platforms have been extensively involved in raising staff cybersecurity awareness programmes though cybersecurity education to students is still largely limited to computing and cyber-related degree initiatives, leaving the rest of the student population with a big gap. However, students' engagement levels vary depending on factors such as course design, self-discipline, and the availability of support services (Jenkins and Slaff, 2020). The ability to monitor student progress through automated assessments and to provide personalized feedback enhances the learning experience and has been associated with improved outcomes (Wang and Chen, 2020).

2.2 Cybersecurity Training

Recent evidence shows that online cybersecurity education is now delivered through several models, including structured e-learning courses, blended activities, distance learning modules and awareness-based interventions. Ahmed et al. (2024) show that universities increasingly use online systems to teach cybersecurity, but Salem, Samara and Al-Tamimi (2024) caution that postgraduate students still experience problems with consistency, technical support and practical depth. Erendor and Yildirim (2022), Raju et al. (2022), Hnaif, Derbas and Almanasra (2024), Verma and Pawar (2024), and Al-Fatlawi (2024) also confirm that student awareness varies across online and distance education settings. These studies support the focus of this thesis because the Bournemouth University case also examines

online training as both an opportunity for scalable education and a challenge for student engagement.

The literature also shows that cybersecurity education should not be restricted to students on technical courses. Salem and Sobaih (2023) argue that cyber hygiene in higher education depends on behavioural and attitudinal factors as well as platform access. Barbu et al. (2023) show that students perceive a range of risks and threats in digital education, while Tazi, Shrestha and Das (2023) highlight privacy, safety and support concerns within online learning structures. These findings strengthen the argument that student cybersecurity training needs to address behaviour, risk perception and platform conditions together.

2.2.1 Technical Training

In today's digital world, almost every student uses the internet, social media, email, and cloud-based tools for learning and communication. This constant online activity exposes them to various cyber threats like phishing, identity theft, and data breaches. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involve the human element, including social engineering attacks and user errors (Verizon, 2023). Cybersecurity training helps students understand how to protect their personal information, recognize suspicious behavior, and follow safe practices online.

2.2.2 Effectiveness of Cybersecurity Training Models

The efficacy of the cybersecurity training models depends on their ability to engage students longer, and enhance the learning outcome of making computing or cybersecurity students in the UK universities be equipped with cybersecurity knowledge and skills to stay aware and prevent cyberattacks. According to Yigit et al. (2024), simulation classes, gamification and virtual labs for cybersecurity training have shown better results for students in retaining cybersecurity skills and enhancing their ability to mitigate cyber threats in the real world. For the students with no previous IT knowledge, it is proven that blended learning models combining online learning with in-person training and hands-on practices have improved their engagement and understanding of critical cybersecurity (Ahmed et al., 2024).

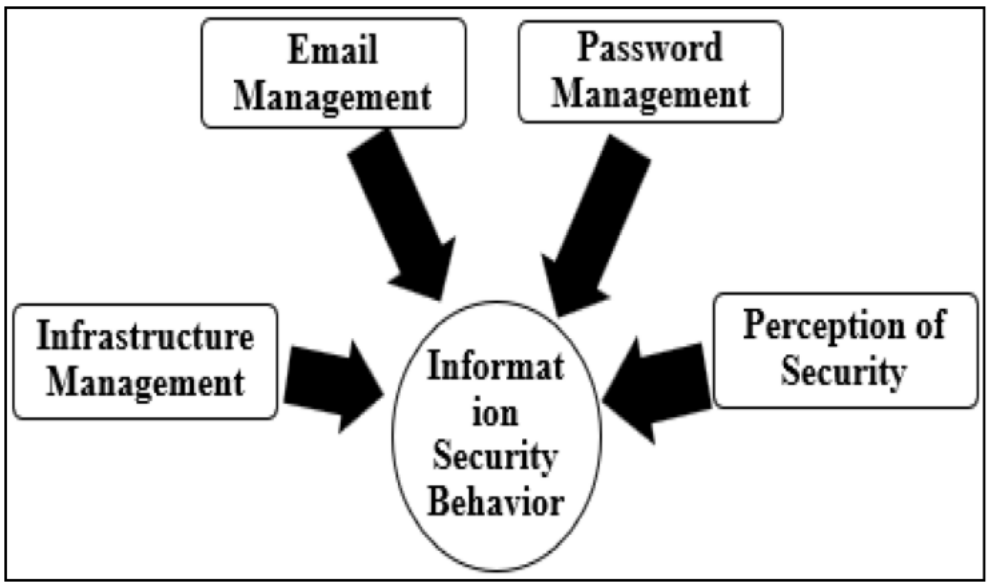


Figure 2: Education, Online Presence and Cybersecurity Implications (Saeed, 2023)

2.2.3 Factors affecting the transfer of training

High-quality content is essential for effective cybersecurity training, with a focus on clarity and depth, ensuring that students acquire both theoretical concepts and practical skills to address real-world cyber threats (Jain et al., 2017). Incorporating real-world scenarios, such as attack and defence simulations, further enhances the transfer of knowledge (Sharma et al., 2021). Active learning through interactive activities, like virtual labs and cyberattack simulations, promotes better retention of knowledge (Kaur and Sharma, 2019), while gamification elements, including badges, points, and leaderboards, increase student motivation and engagement (Huang et al., 2018). However, unequal access to technological resources, such as devices and internet connectivity, can hinder students' ability to engage with online cybersecurity training (Reich, 2020), and technical support is crucial for maintaining a smooth learning experience (Bailey et al., 2021). Learning approaches must account for varying levels of prior knowledge, with tailored content for beginners and advanced learners to improve engagement (Robinson, 2019). Offering diverse content formats, such as videos, articles, and interactive labs, can accommodate different learning preferences (Choi and Lee, 2020). To assess students' readiness, cybersecurity assessments should include practical, problem-solving tasks, such as simulated attacks and incident response exercises, moving beyond traditional quizzes (Garrison and Arbaugh, 2018). Real-time feedback on assignments and quizzes aids in correcting misconceptions promptly (Olsson and Fägerlind, 2017).

2.3 Models of Delivering Cybersecurity Training

A further group of studies demonstrates the value of adaptive, practical and game-based models for cybersecurity learning. Vykopal et al. (2023) emphasise smart adaptive learning environments, while Christensen et al. (2023) demonstrate how game-based platforms can support learning in data protection, privacy and ethics. Prada et al. (2023), Hu (2022), and Nelson and Shoshitaishvili (2024) show that hands-on laboratories and browser-based applied learning can improve practical cybersecurity skills. These sources are relevant because online student training is more likely to be effective when it moves beyond passive content and gives learners opportunities to apply security concepts.

Gamified and challenge-based approaches are also increasingly used in cybersecurity education. Švábenský et al. (2024) describe the movement from paper-based exercises to platform-based learning environments, while Weitl-Harms et al. (2023) and Tay et al. (2024) explain how gamification and capture-the-flag activities can support engagement. Karagiannis et al. (2022), Júnior et al. (2022), Abdiraman et al. (2023), and Paculanan et al. (2024) further show that capture-the-flag and game-based learning can build applied problem-solving skills. This supports the design implication that online cybersecurity training should combine awareness content with more active and realistic learning tasks.

Cybersecurity training for students can be delivered through various methods, each catering to different learning styles and needs. Traditional classroom-based learning provides direct interaction with instructors and peer discussions, fostering a structured environment for foundational learning (Schreiber, 2019). Online learning platforms offer flexibility, allowing students to engage in self-paced learning through modules, quizzes, and virtual labs (Wang and Chen, 2020). Blended learning combines online and in-person sessions, offering a balance of theoretical knowledge and practical application (Thompson and Miller, 2020). Hands-on learning, including simulations, "Capture the Flag" challenges, and virtual labs, is crucial for providing students with real-world experience (Hall, 2021; Green and Becker, 2022). Intensive workshops and bootcamps focus on specific cybersecurity skills, typically in a short, immersive format, to accelerate skill development (Zhao and Xie, 2022). Industry collaboration, through internships and guest lectures, enhances learning by exposing students to real-world challenges and tools used in the field (Schreiber, 2019). Gamification incorporates game elements like challenges and leaderboards to engage students while reinforcing cybersecurity concepts (Hall, 202; Wang and Chen, 2020).

2.4 Advantages of Online Cybersecurity Training

The benefits of online cybersecurity training are strengthened by evidence from recent e-learning and platform studies. Al-Sherideh et al. (2023) show that cybersecurity measures in e-learning can affect students and educators, while Saeed (2023) links online presence with security practices among computing students. Swartz and Nayak (2024) add that cybersecurity education should also respond to intercultural learning needs because students enter online environments with different backgrounds and assumptions. These studies support the thesis argument that online platforms are beneficial when they are scalable, inclusive and context-sensitive, but they also require careful design to avoid treating all students as the same learner group.

Online cybersecurity courses offer several advantages that make them an attractive option for both educational institutions and students. One significant benefit is cost-effectiveness, as online courses reduce the costs typically associated with traditional in-person training, such as venue, travel, and material expenses, making cybersecurity education more affordable and scalable (Al-Bakri et al., 2020). Furthermore, online platforms often include interactive learning tools like simulations, gamification, and real-time quizzes, which enhance student engagement and improve retention of complex cybersecurity concepts. These features provide students with opportunities to practice real-world skills in a controlled, risk-free environment, boosting their learning experience (Khan et al., 2020; Anderson and Tushman, 2020).

2.5 Barriers to Cybersecurity Training

2.5.1 Training needed for cyber professionals or employees, as well as, for students

The ISC2 Cybersecurity Workforce Study found that many professionals enter the cybersecurity field from non-technical backgrounds, highlighting the value of interdisciplinary skills (ISC2, 2022). By receiving cybersecurity training, all students gain a foundational awareness that prepares them to use technology responsibly and safely in both their personal and professional lives. It also encourages critical thinking and risk awareness, which are valuable skills in any field (Center for Internet Security [CIS], 2021). Cyber training is required to address and improve cyber posture, and it is crucial for create first line of defence to resist the cyber attack. Thus, cybersecurity training should not be limited to IT-related fields, students from any discipline will use and rely on digital systems in their future careers. For example, a business student may need to understand how to handle customer data securely, or a healthcare

student must learn to protect patient records. Therefore, introducing cybersecurity training earlier, while they are studying would not only enhance their skills and knowledge, it would enhance their employability.

2.5.2 Requirement for Cybersecurity Training in Higher Education

Training in cybersecurity at universities has become very significant due to the growth of digital infrastructure and the implementation of digital learning systems in universities. Frequently, students and staff access institutional systems, use cloud and personal devices, and these are more vulnerable to cyber threats such as phishing, malware, and data breaches (Hong et al., 2023). One of the predominant causes of security incidents is our human factor and therefore the importance of awareness and behavioural training. Implementation of cybersecurity instruction at the third level continues to safeguard the cyber-practices, aid in operating within the compliance regulations and minimise the organisational risk (Hong et al., 2023). Moreover, cybersecurity education equips students with the relevant skills that are required to operate safely in the environment of the modern electronic environment.

2.5.3 Limitations of delivering Cybersecurity training

Cybersecurity training is important for all students, not just those studying cybersecurity or computing. In today's digital world, almost every student uses the internet, social media, email, and cloud-based tools for learning and communication. This constant online activity exposes them to various cyber threats like phishing, identity theft, and data breaches. According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches involve the human element, including social engineering attacks and user errors (Verizon, 2023). Cybersecurity training helps students understand how to protect their personal information, recognize suspicious behaviour, and follow safe practices online.

2.6 The Need for Cybersecurity Education in Higher Education

2.6.1 Rising Cyber Threats

It has the highest likelihood of a cyberattack targeting universities due to the presence of personal or research information. To safeguard this information, there is a strong need to educate the university community on best cybersecurity practices (Wells and Campbell, 2020). Even though the training in security and cybersecurity aligns more with IT and computing majors, as digital systems are applied across every academic course, students without an

orientation to the technical field are also vulnerable and exposed to cyberattacks. Business, healthcare, education, and social sciences are also associated with routine working with sensitive data and an online platform, and students are vulnerable to threats such as phishing and data leakages.

2.6.2 Digital Literacy as a Core Competency

Beyond specific IT-related fields, digital literacy, including cybersecurity awareness, is increasingly recognised as a core competency for all graduates (Martin, F., and Parker, M. A., 2020). In the growing digital age, digital literacy with proficiency along with cybersecurity skills is becoming essential for students aiming for employment in various industries. This can be achieved by making cybersecurity educators mandatory for all disciplines. Digital literacy is now becoming a graduate-level competency, and it is no longer about the technical skills, but also about the cybersecurity awareness and responsible online behaviour. Cybersecurity training that is based on awareness can be used to help with this competency by providing the students with the requisite information on Microsoft understanding online threats, prudent practises, and institutional roles, and can be efficiently taught on scalable, online learning systems.

2.6.3 Cybersecurity as a regulatory compliance

Data protection rules are strict in higher education institutions, and therefore, compliance is a collective duty of the academic community. Informed staff and student population are the key to the assessment of the regulatory compliance and the risk of data breach reduction (Jones and Simon, 2019). The cost of not adhering to legislation (e.g., General Data Protection Regulation (GDPR)) may result in hefty fines and a tarnished image. As a result, cybersecurity must be seen as a major competency of the entire members of higher education organisations, and not a technical skill only available in specific positions. Staff and student awareness through education of cybersecurity principles will be legal and ethical, encourage best data handling practices and enhance the institutional resilience to cyber threats.

2.7 Personal Factors

There are personal factors that may influence students' cybersecurity awareness and behaviour. Personal attributes, such as internet use trends, risk awareness, self-confidence, and online behaviour, determine how students approach online systems and the likelihood that they will respond to potential dangers. For example, students who have had high levels of

problematic internet use may eventually get desensitised to online risks, whose probability would be developing towards unsafe digital behaviours is high.

2.8 Behavioural Traits

The behavioural characteristics play an important role in determining the manner in which the students interact with the cybersecurity practices and avoid online threats. Impulsivity, risk-taking behaviour, and complacency regarding security issues are traits that may lead students to ignore security warnings, use weak passwords, or open links that appear suspicious (Zulkiplee et al., 2025). An interpretation of behavioural traits is relevant to the design of specific cybersecurity training that stimulates desirable security behaviours and enhances cyber overall performance.

2.8.1 Security Behaviour Intentions

Security behaviour intentions describe how an individual is willing to perform safe cybersecurity behaviours, including strong passwords, multi-factor authentication and acting in a proper way to security warnings. Measurement of these intentions is usually done by use of Security Behaviour Intentions Scale (SEBIS) which is a validated tool to measure the disposition of users to use protective online computer behaviours (Egelman and Peer, 2015).

2.8.2 Problematic Internet Use

Problematic Internet Use (PIU) refers to excessive or compulsive use of Internet activities that have the potential to lead to self-regulation lapse and exert more exposure to cyber threats. PIU is usually determined by validated scale surveys; these include Problematic Internet Use Scale that measures behavioural dependency, loss of control as well as risky online behaviours related to increase in vulnerability (Demetrovics et al., 2016; Coutlee et al., 2014)

3 METHODOLOGY

3.1 Introduction

This chapter expounded the methodological approach which will be used in studying the barriers and advantages of online platform use in training students on cybersecurity. The aim of the study was to investigate the nature of the relationships between problematic internet use, impulsiveness, intentions of security behaviours and cyber performance in a higher education environment. Methodology presents the reasoning, which links the research problem, philosophical assumptions, design choice, data source and procedures of analysis, given that it makes a study cohesive and believable. The methodology in this study matched the quantitative measurement of behavioural variables and statistical correlations of them within a real institutional setting. The chapter thus talks about the research philosophy, mode of reasoning, research design, method of data collection, method of data analysis and ethical issues and summary of the chapter. It also explains why quantitative case study using secondary data based on KnowBe4 pilot programme at Bournemouth University was suitable in providing the answer to the research questions and posing the hypotheses.

3.2 Theoretical Framework

The theoretical framework developed in the context of the study was based on the hypothesis that students with particular behavioural characteristics can be more interested in approaching online training on cybersecurity and demonstrate high performance on online learning challenges that are cyber-related. It was based on data provided by the pre-test surveys filled by students prior to taking the cybersecurity modules on Brightspace. Such surveys were developed to indicate three behavioural constructs which included problematic use of the internet, impulsivity and security behaviour intentions. The pre-training behavioural measurements, as Sussman and Leavitt (2023) suggest, can be an effective approach to how the current habits of the learners, their self-regulation, and the digital behavioural patterns might affect engagement and receptiveness in online learning activities. The framework in this study placed these behavioural traits therefore as the explanatory variables which may contribute to the engagement in the training modules, and cyber performance results.

The framework based itself on scales that have been tested and validated to operationalise the major constructs. There was problematic internet use assessed with PIU scale (Demetrovics et al., 2016), impulsivity assessed with Abbreviated Impulsiveness Scale or ABIS (Coutlee et al., 2014) and security behaviour intentions assessed with SEBIS (Egelman and Peer, 2015). These precautions helped the study to investigate the relationship of internet dependency, impulsive behavior and prevailing security habit among students engaging on and achieving in online training of cybersecurity. Previous studies indicate that dysfunctional internet usage could be connected to less strong self-regulation and less safe online behaviour and hence diminish secure digital practices (Caplan, 2010; Hadlington, 2017). In the same vein, hasty decision-making and reduced compliance with cybersecurity measures have also been linked to impulsivity and can adversely influence secure behaviour (Coutlee et al., 2014; Aivazpour and Rao, 2022). Simultaneously, the improved security behaviour intentions should underpin the safer online behaviour and enhanced training performance (Egelman and Peer, 2015; Moustafa et al., 2021).

Based on this framework, three hypotheses were developed.

- H1 proposed that higher levels of problematic internet use would negatively affect security behaviour intentions.
- H2 proposed that higher impulsiveness would negatively affect security behaviour intentions.
- H3 proposed that student cyber performance would be influenced by security behaviour intentions, impulsiveness, and problematic internet use.

Together, this framework provided a clear conceptual basis for examining how individual student traits shaped cybersecurity learning within the university case study context.

3.3 Research Philosophy

Research philosophy is the group of assumptions regarding the knowledge, the reality as well as how the valid evidence is to be produced in a study. The philosophy directs the opinion of a researcher regarding what is considered knowledge and the way it can be achieved as Nayak and Singh (2021), Patel and Patel (2019), and Ragab and Arisha (2018) explain. Snyder (2019) also observes that the methodology is inevitably chosen as the philosophical stance that supports the study since the latter determines the pattern of inquiry, evidence and interpretation. The philosophical position in this study must have justified the

systematic discussion of the relations between the measurable variables, but not the pursuit of subjective meanings by explanations in terms of narratives.

According to Pervin and Mokhtar (2022), a paradigm can be defined as a basic set of beliefs that direct the action, and this is most likely to be determined by the disciplinary background, experiences, and assumptions of the researcher. It implies that a philosophical worldview introduced by a researcher results in the choice of approach to a study, and that worldview also needs to be provided since it affects the entire course of research (Alharahsheh et al., 2020).

The paradigm in this study was based on positivism. Positivism is based on the assumption that there is a world of reality that is beyond the researcher and there is a possibility that valid knowledge can be generated by means of empirical observation, measurements and testing of variable relationships. According to Alharahsheh and Pius (2020), positivist inquiry is especially the most appropriate in situations when the aim of research is to be tested and define relationships based on visible evidence. This study was applicable to the current research as it examined the statistical relationships between problematic internet use, impulsiveness and security behaviour intentions and cyber performance in cybersecurity training over the internet.

Positivism enabled the researcher to shift the focus away on theory to testable hypotheses as well as testable hypotheses to statistical evidence. Such philosophy fits perfectly well with studies that seek to produce evidence-based evidence that can inform decision-making, policy, and intervention as proposed by Patel and Patel (2019) and Nayak and Singh (2021). It is on this basis that the research philosophy gave a solid rationale towards the deductive, quantitative and case based methodological decisions adopted in conducting the research.

3.4 Mode of Reasoning

Modes of reasoning can be defined as the logical process that the researcher takes in order to tie theory and evidence. According to Acharyya and Bhattacharya (2019), research reasoning usually entails an inductive or deductive process, the latter being offered when the research generates a theory out of data and tests a theory based on empirical evidence. Deductive reasoning is also characterized by Bairagi and Munot (2019) as a process that starts with an idea or a set of ideas (conceptual propositions) based on already known information, and analyzes the truth or falsity of such propositions in observed data. According to Basias and Pollalis (2018), deductive reasoning is the most appropriate method

when the study aims to confirm the already known constructs and relationships with the help of a structured analysis.

A deductive mode of thinking was applied in this study. The study has started with the current literature on cybersecurity behaviour, problematic internet use, impulsive, online learning behaviour and student cyber performance. Based on this literature foundation, the researcher came up with theoretical predictions on the roles of particular behavioural characteristics on secure internet behaviour and the results of training. Research questions and formal hypotheses were generated based on these expectations. The hypotheses were the following: an increased problematic internet use would be negatively correlated with the security behaviour intentions, an increased impulsivity would decrease the security behaviour intentions and behavioural traits would play a role in cyber performance. These propositions were not formulated through the open-ended field observation, but the propositions came into being by a set of theoretical arguments and previous empirical studies and then tested by use of numerical data.

concentration in the analysis since every phase of the research was interconnected to its initial research objectives. It was also in favour of consistency between the positivist research philosophy and the quantitative design, where they both are in favour of structured inquiry and evidence based conclusions. Thus, the logic of this study was deductive and enabled the researcher to check theory-informed anticipations in an actual university by systematic quantitative carrying out of the research.

3.5 Research Design

Research design gives the general account of how a research will answer its research questions in a logical, systematic, and credible manner. It directs the organisation of evidence, the analysis of variables, and the methodology selection is justified to address the goals of the research. Research design is not merely a technical selection as Gupta and Gupta (2022), Kapur (2018), Kumar (2018), and Kumari et al. (2023) explain: it is a framework that connects the aim of the research with the ways to obtain valid conclusions. The key design types in social research are mixed-methods, quantitative, and qualitative. Qualitative designs are usually employed when the researcher is interested in learning about perceptions, lived experiences, and the meanings at a deep level, which may be achieved using a flexible sort of approach and interpretive analysis. In one instance, phenomenological research is narrower in that it is interested in the experience that the participants have of a given phenomenon and

how the experience can be interpreted based on their point-of-view (Greening, 2019). In comparison, quantitative design is focused on measurement, comparison, variables relationships, and hypothesis testing using structured numerical data (Kumar, 2018; Gupta and Gupta, 2022).

This paper used a quantitative case study design. The study was quantitative as the researcher aimed to test quantifiable relationships between behavioural variables and cybersecurity training outcomes and not investigate subjective experiences via interviews or stories. The researchers questioned the relationships between problematic internet use, impulsiveness and security behaviour intentions and engagement and cyber performance among students. The validated scales could be used to operationalise these constructs and the data could be statistically analysed making a quantitative design the best option. This methodology aligned with the research questions, which necessitated the comparison of groups, the establishment of relationships, and establishment of relationships that are predictive by measuring indicators. It also facilitated the research goals as a number of variables could be analysed collectively, such as behavioural characteristics, demographic analyses, engagement behaviours, and performance outcomes (Kapur, 2018; Kumari et al., 2023).

Meanwhile, the research was intended to be carried out as a single-case study due to the focus on one limited system of institutions: the cybersecurity awareness training programme provided to the students of Bournemouth University using KnowBe4 and Brightspace. The case study design was appropriate as the study enabled the researcher to explore a modern phenomenon in actual situation, where context and behaviour issues were significant. The overall case in this instance was the university training programme, with the unit of analysis being the individual student, which was embedded in it. This design enabled the investigation of the effects of behavioural traits on the results of a realistic online training setup. Thus, the research approach combined the strengths of quantitative methods with the contextual elaboration of a single-case study design, whose results were organized, applied to practice, and based on the context of educational cybersecurity in institutions.

Table 1: Alignment of Research Design with Study Components

Study component	**Methodological choice**	**Relevance to this study**

Philosophical orientation	Positivist	Supported objective measurement and hypothesis testing
Mode of reasoning	Deductive	Enabled theory-led development of hypotheses
Research approach	Quantitative	Allowed statistical analysis of behavioural variables
Design context	Case study	Examined a real university cybersecurity training setting
Unit of analysis	Individual student	Focused on student traits, engagement, and performance

3.6 Data Collection Method

Data collection Method is defined as the method through which get the evidence to respond the research questions. Kumar (2018), Kumari et al. (2023), Mishra and Alok (2022), and Mahuika and Mahuika (2020) note that the suitability of the data collection approach depends on the character of the research problem, access to data, and the type of analysis intended. Secondary data was collected in the current research. It implies that the study did not involve collecting new data directly with the participants; rather, it used the already existing data created by the KnowBe4 pilot project at Bournemouth University. Secondary data collection was appropriate since the purpose of the study was to examine the patterns and relationships which were already recorded in a structured dataset and the dataset had the precise variables Desired in the analysis.

Data transposed in this case study was acquired in cybersecurity awareness training programme through Brightspace being the virtual learning of Bournemouth University in partnership with KnowBe4. Under the programme, about 18,000 students were given seven voluntary trainings on cybersecurity. The students were given pre-test survey aimed at evaluating their nature of behaviour before participating in the training. These surveys accommodated instruments of problematic internet use, impulsiveness, and security behaviour intentions that are validated. Sussman and Leavitt (2023) argue that this type of pre-test measures can be effective at identifying behaviours that could influence the engagement and responses of a learner to digital security interventions. The pilot programme produced a final sample of 544 current students and alumni that took all pre-training survey and training modules.

It was fitting to use secondary data due to a number of reasons. Firstly, the variables were already organized using the variables that made the fundamental aspect of the study and consequently it was feasible to look into the study questions directly. Secondly, the information was based on an actual intervention at an institution, making the study more practical as well. Third, secondary data minimized time and logistical requirements of gathering massive amounts of primary data and also enabled a rigorous analysis. The protocol used in the case study enhanced the process of collection by defining the problem, unit of analysis, research questions and hypotheses. The unit of analysis used in the present study was the individual student since the study involved the effect of personal behavioural traits on engagement and cyber-related consequences of training.

Chapter 1 initially introduced the research questions that the research was based on and looked at how behavioural traits and subject area impacted the use of cybersecurity training by students and their completion. These constructs have been operationalised using the data of the pilot study with the help of the validated scales. The researcher sought to establish whether and how individual students behavioural characteristics influenced attendance of, or completion of training modules by utilising prior reliable measures of PIU, ABIS and SEBIS. The hypotheses were also informed by prior literature on problematic internet use, impulsiveness, cybersecurity behaviour, and online engagement (LaRose et al., 2010; Caplan, 2010; Hadlington, 2017; Ng et al., 2020; Sussman and Leavitt, 2023; Zhao and Xie, 2022).

Table 2: Overview of Dataset Used in the Study

Dataset feature	**Description**
Source	KnowBe4 pilot study at Bournemouth University
Platform	Brightspace VLE
Target population	BU students and alumni
Final dataset size	544 participants
Nature of data	Secondary quantitative data
Key variables	PIU, ABIS, SEBIS, demographics, engagement, performance
Unit of analysis	Individual student

3.7 Data Analysis Technique

In this study, statistical analysis, as applied in JASP software was used to perform data analysis. As the data used was quantitative in nature, it was assumed that numerical

analysis was the most appropriate means to study the relationships between the variables as well as test the hypotheses formulated. According to Mishra and Alok (2022), Mukherjee (2019), Nayak and Singh (2021), and Patel and Patel (2019), the quantitative data analysis method is valid when a researcher is interested in identifying patterns, comparing groups, estimating relations, and producing evidences based on objective methods. Though Mohajan (2018) is writing on the topic of qualitative research, indirectly, he justified the argument that quantitative analytical methods are more suitable in case the intention is to measure and test statistically and not in order to gain a deeper and more accurate comprehension.

In this work, the analysis was conducted in the past tense since the processes had already been implemented on the available data. To ascertain the internal consistency of items in the PIU, ABC, and SEBIS scales, first, Cronbach alpha was used to establish reliability of the measurement tools. This was needed since unless there are reliable scales, it can be impossible to come up with credible conclusions out of composite measures. After establishing acceptable levels of reliability, composite scores in the behavioural constructs were derived. These scores were then used in subsequent analyses.

The sample characteristics (gender, level of study, faculty and age categories) were summarized using descriptive statistics. Correlation of all the above main variables especially problematic internet use, impulsiveness, security behaviour intentions and performance was then done to identify the direction and strength of the association between the two variables. Regression analysis was used to determine the predictive relationships outlined in the hypotheses. Furthermore, inferential statistics like independent samples t-tests and one-way ANOVA were employed appropriately to make comparisons, like between groups, such as between subject areas and age groups. These methods were appropriate because the research was interested in identifying whether variables correlated as well as whether there was a significant variation of variables among cohorts of students.

JASP was chosen as it offered convenient interface to analyse behavioural and social sciences, and supports the entire range of necessary tests. Structured statistical procedures enhanced the levels of transparency, replicability, and conformability to the positivist paradigm. The analytical approach thus enabled the researcher to make a transition between reliability analysis to descriptive profiling up to hypothesis testing in a logical progression.

Table 3: Data Analysis Techniques Used

Technique	Purpose in the study
Cronbach's alpha	Tested internal consistency of PIU, ABIS, and SEBIS scales
Descriptive statistics	Summarised participant characteristics and key variables
Correlation analysis	Examined associations between behavioural constructs and performance
Regression analysis	Tested predictive relationships in the hypotheses
Independent samples t-test	Compared selected student groups
One-way ANOVA	Examined differences across multiple categories such as age

3.8 Ethical Considerations

Ethics was also a crucial factor since the research used data of human participants although this was not primary data but secondarily gathered by the researcher at hand. This research was approved by the Bournemouth University Ethics Committees and the initial KnowBe4 pilot research had already received full ethical approval prior to the start of the data collection using the Ethics Reference No. 52345. The current study thus secondary utilized an approved dataset, which enhanced ethical considerations.

The sample included data of 544 Bournemouth University students and alumni who have willingly attended the cybersecurity awareness programme and taken both pre-training survey and training modules. Since the information was derived in an already existing institutional study, the researcher was required to maintain the consistency of the reuse with previous ethical consent, confidentiality requirements and purpose of the research. There was no new participant contact and no primary data collection had been carried out. The data were considered a secret and the data were applied solely to the academic purposes and interpreted in the aggregate manner and it was not possible to identify individual persons. A certain amount of ethical care was also necessary since such behavioural characteristics as problematic internet use and impulsiveness were involved in the study and might be quite sensitive when reported in a manner that might stigmatise individuals or groups of people. The researcher thus tried to research on patterns and relationships as opposed to personal judgement.

Methodological integrity was also a concern of ethics in this study. Validated scales, a well-defined case study protocol, and careful analytical procedures conferred fairness,

credibility, and conscientious interpretation. Moreover, the researcher was not unmindful of the fact that the sample was also selected as a result of a voluntary training programme and thus findings needed to be communicated carefully without overemphasising the generalisability out of the study context. Ethical research thus went beyond the approval to refer to responsible management, analysis and reporting of the data during the study.

3.9 Summary of Chapter

The chapter has discussed the methodological framework applied to explore the issues and advantages of online platform in training students on cybersecurity. It determined that a positivist philosophical stance formed the basis of the study that reflected the perception that social phenomena could be analyzed based on objective measurement, hypothesis testing, and statistical evidence. The notion that a paradigm is comprised of beliefs that determine action and influence the research process supported that position (Pervin and Mokhtar, 2022; Alharahsheh et al., 2020).

This study used a quantitative research design and a real-world case study of the KnowBe4 pilot programme at Bournemouth University that is implemented using Brightspace. This research design was appropriate since the various outcome measures that were researched included behavioural variables that were measurable such as problematic internet use, impulsiveness, security behaviour intentions, and cyber performance. The context of the case study provided both practical and institutional relevance as it enabled the researcher to analyse the relationships within a limited university environment. The chapter also explains that the research has been based on secondary quantitative data of 544 students and alumni who had volunteered to join the training programme and went through the corresponding pre-test surveys.

4 ANALYSIS

4.1 Introduction

This chapter introduces and addresses the findings of the quantitative case study of the cybersecurity student trainings on online platforms. The secondary data set from the Bournemouth University KnowBe4 pilot study was analysed as part of the project that was conducted in Brightspace. The chapter maintains its focus on the variables set out in the methodology. The following variables are analyzed: Problematic Internet Use, the Abbreviated Impulsiveness Scale, Security Behaviour Intentions, demographic characteristics, engagement, and cyber performance. The aim is not just to provide value relating to statistics. Secondarily, the intent is to elucidate the meaning of these values in the context of online cybersecurity training in a university environment.

The logic of the hypotheses is adhered to in the chapter. It first has to analyze the reliability of the scales since reliable measurement is required prior to any useful interpretation. This follows by introducing the demographic profile of the participants raised as the findings are dependent on composition of the sample which can influence their strength and limit. The same analysis is followed by the behavioural traits analysis and correlation. Each hypothesis is tested in the last sections and the findings are discussed to answer the research questions. This structure is based on the concern that the results should actually convey a story instead of presenting individual statistical tests.

The chapter has been based on 544 valid responses from current Bournemouth University students and alumni. The data were collected as part of the earlier pilot study. Students were asked to complete a pre-training questionnaire before participating in cybersecurity training programs. To assess the questionnaire's content, three behavioural scales were used. The Problematic Internet Use scale from Demetrovics et al. (2016), Abbreviated Impulsiveness Scale from Coutlee et al. (2014), and the Security Behaviour Intentions Scale from Egelman and Peer (2015). These scales enabled the study to explore the relationship between student's behavior prior to the training and security intentions and cyber performance. Thus, the analysis was directly related to the theoretical framework and the design of the case study problem as discussed in Chapter 3.

4.2 Reliability and Measurement Quality

Prior to the primary analysis of data reliability was analyzed. This was required because this study relied upon composite scores for PIU, ABIS and SEBIS. It is desirable that the internal consistency of the items in these scales should be adequate otherwise, the regression or correlation analysis would be regarded less credibly later on. A common index for quantitative research used the Cronbach's alpha. Tavakol and Dennick (2011) indicate that if the alpha is > or near .70 the researcher will typically declare it acceptable however the researcher should also take into account the number of items and the type of construct under examination. This warning is important because not all behaviours have simple or simply uniform dimensions amenable to being measured using scales.

Table 4: Reliability Analysis

Variable	Cronbach's Alpha	Number of Items	Interpretation
Problematic Internet Use	0.778	6	Acceptable internal consistency
Abbreviated Impulsiveness Scale	0.861	13	Good internal consistency
Security Behaviour Intentions Scale	0.757	16	Acceptable internal consistency

As can be seen from Table 4 all three measures had the anticipated level of reliability. The internal consistency of the six items of the PIU scale was acceptable with an alpha score of 0.778. This indicated that the objects were sufficiently related for the purpose of using them as a composite index of problematic Internet use. The highest reliability was obtained from the ABIS scale; 0.861 (alpha) with 13 items. This indicates a good internal consistency of the impulsiveness scale in this data set. The SEBIS scale yielded an alpha coefficient of 0.757 over 16 items, with also support from that scale for being a composite indicator of security behaviour intentions.

The findings obtained for reliability are important since they indicate that there were enough consistencies across the three behavioural constructs measured to justify further analysis. This isn't to say that the scales are flawless. It indicates that the answers were coherent enough to be able to average or composite scores. As the scores were reliable, students could now be compared, test/behavioural patterns could be interpreted more reliably and structured. It is of great practical importance that the result confirms the use of validated scales in practical research in the field of cybersecurity in online training. There is a need for tools to measure tendencies like risky Internet use, impulsive decision making and security

intention with reasonable consistency, a need that universities interested in understanding student behaviour need.

The reliability findings are another positive justification for the use of a quantitative case study. There was no reliance on generalized impression of engagement. It employed structured survey instruments that have a quality test on an internal basis. This will help to make the results easier to understand. It also contributes to the linkage of results gained in the study to the broader research on cybersecurity education. Behaviours that were discussed in earlier research such as those related to PIU, ABIS and SEBIS were used in the current research, as they have been used in other similar behavioural studies, but in the context of Bournemouth University's online cyber security training programme.

4.3 Age Distribution of Respondents

The demographic section provides background to the statistical results. It depicts the number of people included in the sample and where caution needs to be used when making conclusions from the results. Students who participated in the pilot programme were offered this course, however a much larger number of students (544 completed and valid data for this course) were considered. A number of responses were excluded because of missing data. The total score variable had a smaller number of participants, 363, who answered everything for this question. This resulted in some analyses being performed with varying amounts of usable data. This is a typical problem of second hand quantitative datasets and should be taken into account in the results interpretation.

Table 5: Gender Distribution

Gender	Frequency	Percentage
Male	220	40.4%
Female	300	55.1%
Alumni (Non binary/ not specified)	24	4.5%
Total	544	100%

From Table 5, it shows that the gender difference to the samples was relatively even with majority women accounting 55.1%, while men accounted 40.4% of all the respondents were male; 4.5% of Alumni students. This distribution indicates that the sample is not restricted to one gender group. The gender profile, however, should be viewed with caution as the study was not primarily examining gender as the primary explanatory factor. Gender was not the main theoretical proposition, but rather part of a larger group of demographics.

Figure: 3

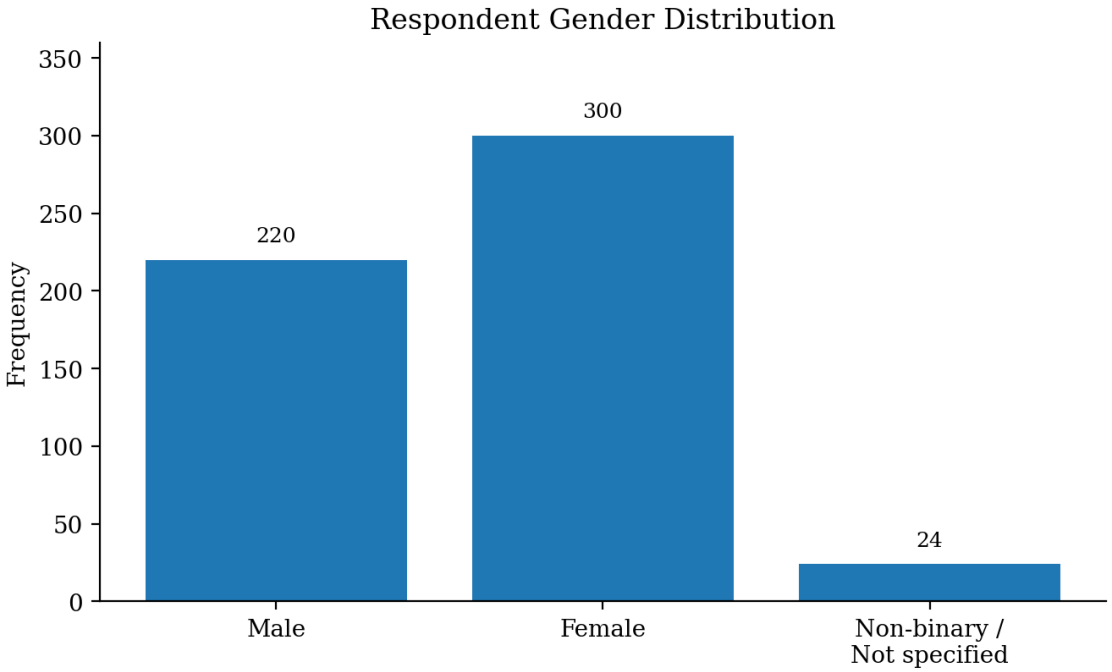


Table 6: Level of Study

Level	Frequency	Percentage
L4	163	30%
L5	136	25%
L6	82	15%
L7	109	20%
Alumni	27	5%
Total	554	100%

According to Table 6, the majority of students who participated were at level 4. This indicates greater representation of early-stage students. There were also students at L5, Level 6 and L7 (in smaller numbers). The smallest group was made up of alumni. The table breaks responses into level categories and includes a total value larger than the valid responses count due to the recording of the level categories in the data set. It should not be overlooked and is actually a data quality problem. It suggests that the use of demographic variables should be considered for context, but that these should not be viewed as value-free variables.

Figure: 4

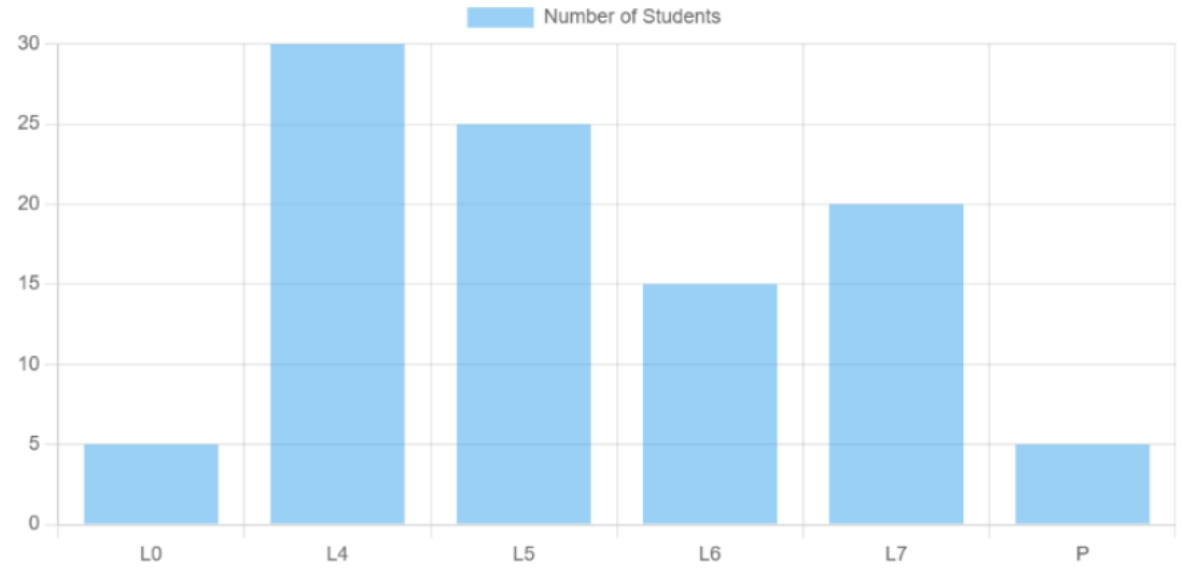
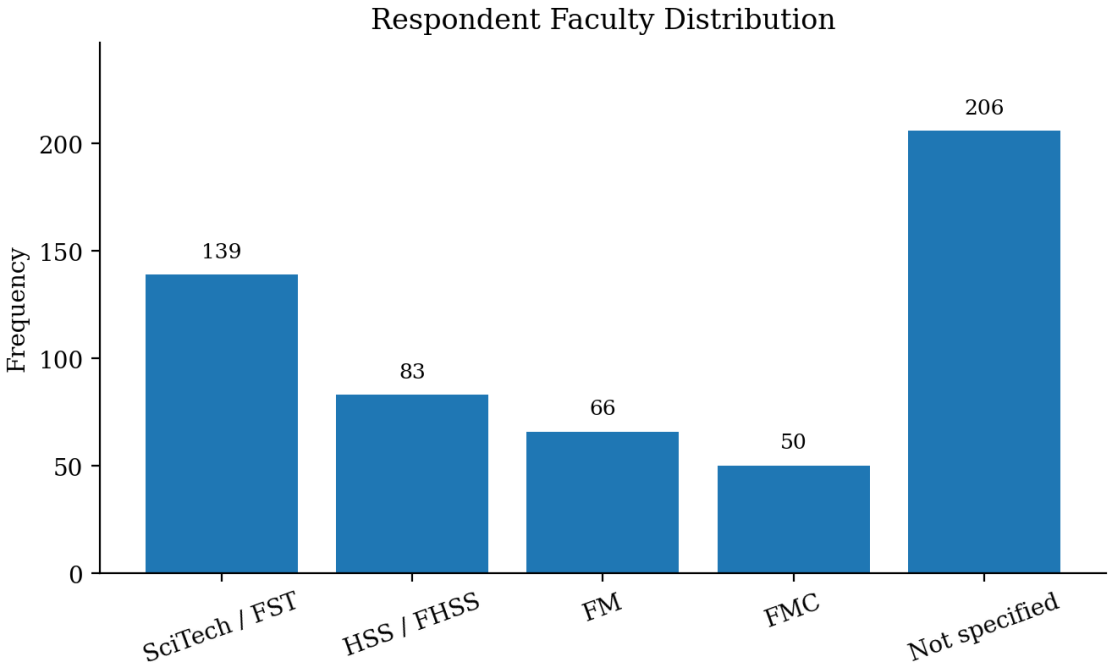


Table 7: Faculty Distribution

Faculty	Frequency	Percentage
SciTech or FST	139	25.6%
HSS or FHSS	83	15.3%
FM	66	12.1%
FMC	50	9.2%
Alumni	206	37.9%
Total	544	100%

There is a significant amount of missing or unspecified information about faculties in Table 7 Alumni accounted for the largest number of cases at 37.9% of the sample. The highest percentage was 25.6% from the specified faculties, of which SciTech was the biggest. It is important because students in the technology-related fields may be expected to have a greater motivation for cybersecurity training. The absence of faculty results, however, prevents meaningful inference about differences between disciplines. However, the sample indicates that students from a number of academic areas engage in training programmes, but does not provide strong evidence for an oversimplified claim that students from one faculty did better than those from another.

Figure: 5



One of the key arguments of the thesis is supported by the demographic pattern. Educating students about cybersecurity shouldn't be a sole responsibility of computing students. Students from various levels and faculties of the dataset. All students utilize digital systems, utilize cloud platforms, send and receive email and use the University network is a reflection of this institutional reality. Demographic responses thus also confirm the need for wide cybersecurity awareness training across the entire University community. The uneven and incomplete demographic profile also indicates that the data captured in online training programmes must be improved to enable accurate data on which future decisions may be made.

4.4 Behavioural Traits and Correlation Results

Correlation Analysis focused on the direction and strength of relationships between raw performance score, PIUQ and ABISQ/SEBISQ. Importance of this analysis: It gives an initial picture of the relationships between the behavioural variables, in the absence of the formal hypothesis testing. The correlation isn't causation. It indicates whether two variables tend to go in the same or opposite direction. Most significant was this Relationship between problematic internet use and security behaviour intention since it was directly related to the first hypothesis.

Table 8: Pearson Correlations Among Main Variables

Relationship	Pearson r	p-value	Interpretation
ScoreRaw and PIUQ	-0.021	0.703	Not significant
ScoreRaw and ABISQ	0.080	0.149	Not significant
ScoreRaw and SEBISQ	0.023	0.680	Not significant
PIUQ and ABISQ	-0.237	< .001	Significant negative relationship
PIUQ and SEBISQ	-0.408	< .001	Significant negative relationship
ABISQ and SEBISQ	0.241	< .001	Significant positive relationship

The results presented in Table 8 indicate that there is a significant negative correlation between problematic Internet use and intentions for security behaviour. The correlation value was $r = -0.408$ with $p < .001$. This indicates that students who scored higher on problematic behaviours scale tended to have lower intentions of security behaviours. Theoretically, the result will validate unregulated or compulsive internet use theory of decreased careful online behaviour. It also demonstrates that PIU is not merely ‘wellbeing' issue. It may also be applicable to the field of cybersecurity education, as individuals who have difficulties with self-regulation of internet use may be less inclined to make robust intentions to engage in safe online behaviors.

There was a positive relationship between ABISQ and SEBISQ, $r = 0.241$, $p < .001$. This result is more complicated in that the hypothesis predicted impulsiveness to have a negative relationship with aspects of security behaviour intentions. This positive trend indicates that in this data set, students with higher impulsiveness didn't necessarily indicate lower levels of security intentions. This could be because students with more impulsive tendencies are able to identify safe behaviour when it is queried in a survey. Another view is that the intentions of an individual regarding security are not exactly congruent with their actual behaviour. Students might mean well but act hastily or recklessly in real digital contexts. The difference does not come up much in cyber security training as awareness is not sufficient for practical safety.

There was also a significant and negative relationship between PIUQ and ABISQ ($r = -.237$, $p < .001$). However, this result is not what one might have expected based on the notion that problematic Internet use and impulsiveness go hand in hand. This may be due to the nature of this sample and/or the manner in which variables were measured. It can also mean

that problematic Internet use and dependent behaviour/internet addiction are habit-based behaviors and impulsiveness refers to fast acting but without planning. These are similar behavioural problems not the same. This reinforces the thesis that student behaviour should not be lumped together and treated as a single type of training in cybersecurity training in the online environment. Various behaviour traits may require varying training responses.

The correlation table did not reveal any significant relationships between the raw performance score and PIUQ, ABISQ, or SEBISQ. It implies that cyberself-efficacy was not well predicted by any single behavioural construct. This is crucial since it avoids sole relying on the information to make an over-eager decision. While behavioural traits seem to be effective to understand security intentions, other factors could influence cyber performance. They can be knowledge, module design, motivation, technical familiarity, time available for training, etc., and to a great extent, participation may be voluntary. The outcome thus serves as a basis for a well-rounded presentation of cybersecurity lessons learned through digital applications, both good and bad.

4.5 Hypothesis 1: Problematic Internet Use and Security Behaviour Intentions

The first hypothesis suggested that students with higher problematic internet use scores would exhibit weaker intentions to engage in security behaviour. This hypothesis was confirmed with regression analysis. The model adequately accounted for 16.7% of the variance in the SEBISQ sample. The model was statistically significant ($F = 94.911$, $p < .001$). The standardised coefficient was negative (beta =- 0.408) and $p<0.001$. This clearly demonstrates that having problematic Internet use was a significant predictor of the sample's attitudes toward security behavior.

Table 9: Regression Result for H1

Statistic	Value	Meaning
R	0.408	Moderate relationship
R squared	0.167	PIU explains 16.7% of SEBIS variance
Adjusted R squared	0.165	Stable explanatory value
F statistic	94.911	Model is statistically significant
p-value	< .001	Relationship is significant
Standardised beta for PIUQ	-0.408	Higher PIU predicts lower SEBIS

The outcome narrates a straight-forward story on student actions with respect to online cyber security training. Students also indicated that they were more likely to report

difficulties with managing their Internet-related activities and less likely to adopt secure practices online if they had greater difficulties with managing their Internet use. This research finding takes place in the theoretical context of the study. Difficulty self-regulating, frequency of access to unsafe online environments, and attending to warnings poorly. These inclinations can assist students not to recognize or utilize secure behaviour, even if expertise is offered. In the world of online cybersecurity education, there is more to it than just delivery of learning materials. The platform could offer modules, quizzes, and information, but the learner's digital behaviour may make it more or less likely that it would result in secure intentions.

It also ties in to the challenge aspect of the research topic. Platforms are accessible to online but much depends on the amount of student self-management. Where students demonstrate internet habits that may be problematic in itself then they may not be 'mindful' readers of training information. They might finish the modules in a rush, do not reflect on, or don't relate the module content to their own hands-on practice. This puts a constraint on the online cybersecurity training. It can impact on the number of students but not necessarily all pupils. Students who receive the higher PIU might require extra prompts, shorter learning segments, reminders and/or reflective activities to link to everyday online behaviours.

The H1 result is also good for universities. It proposes that, in addition to technical security rules, cyber security training should involve information on self-regulation and digital wellbeing. A student, who knows what phishing is in theory, could still click on an unsafe link if he/she acts (online) in a hurried, distracted, and unruly manner. Such a negative correlation between PIU and SEBIS thus creates the basis in cybersecurity education for a more behaviour based approach. The purpose of training shouldn't be to just explain what to do to the pupils. It should encourage students to understand the impact of the Internet use habits on their security decisions. This will help to make online training more relevant and more likely to impact real behaviours.

4.5.1 Academic Discipline and Security Behaviour Intentions

The researcher then analysed any differences between computer science and non-computer science students regarding security behaviour intentions. In independent samples t test, there was no significant difference ($p = 0.695$). Which implies that there was no evidence regarding the difference in computing student security behaviour intentions compared to non-computing student security behaviour intentions in this data set. It is a

significant discovery as it suggests there is a potential disconnect between students' security intentions and their actions in technical courses.

Table 10: Independent Samples T-Test for SEBIS by Department Group

Measure	t	df	p-value	Cohen's d	Interpretation
SEBISQ	-0.393	493	0.695	-0.055	No significant group difference

The finding supports the argument that cybersecurity training should be provided across the whole student population. Technical knowledge may help students understand cybersecurity concepts, but it does not guarantee stronger intention to follow secure practices. The absence of a significant difference also supports the case for inclusive training. Business, health, media, social science, and technology students all use digital systems. All are exposed to phishing, weak passwords, unsafe downloads, and data handling risks. Therefore, universities should not assume that security behaviour is only a concern for non-technical students or only a skill for computing students.

4.5.2 Age Group and Security Behaviour Intentions

The analysis also examined whether security behaviour intentions differed among age groups. The one-way ANOVA showed a significant difference, with $F = 5.570$ and $p = 0.004$. This result indicates that age had some relationship with security behaviour intentions. The reported interpretation suggested that students aged 35 and above displayed stronger security behaviour intentions than younger groups. This finding may reflect maturity, work experience, greater awareness of risk, or stronger responsibility in digital decision making.

Table 11: One-Way ANOVA for SEBIS by Age Group

Source	Sum of Squares	df	Mean Square	F	p-value
Age	3.154	2	1.577	5.570	0.004
Residuals	139.275	492	0.283		

This age result enriches that of H1 as it indicates that intentions to be secure are not determined solely by one behavioural variable. The student's age can affect his/her perception of cybersecurity threats and attitude towards the adoption of safe practices. Students can have intimate knowledge of a digital platform, but that does not necessarily mean they are cautious. More experienced older students might already have personal experience of the rules of the workplace or financial risks or data protection duties. This may indicate a need for some personalization of online training. For younger students, a more concrete model,

simulation, and instant feedback might be helpful. Older students can be responsive to policy, compliance, and business risks scenarios. This can be facilitated through the use of online platforms as the content can be adapted to serve a variety of groups, and this adaptation needs to be deliberately designed.

4.6 Hypothesis 2: Impulsiveness and Security Behaviour Intentions

The second hypothesis suggested that impulsiveness will be negatively correlated with security behaviour intention. The hypothesis in this direction was not supported by the results. According to this regression result ABISQ had a positive relationship with SEBISQ which was statistically significant. There was an estimated R squared of 0.058 and $p < .001$ for the model explaining security behaviour intentions; the model explained 5.8% of the variance. As per the standardised beta, the greater the value of impulsiveness, the higher the reported security behaviour intentions in this dataset will be.

Table 12: Regression Result for H2

Statistic	Value	Meaning
R	0.241	Weak positive relationship
R squared	0.058	ABIS explains 5.8% of SEBIS variance
F statistic	28.068	Model is statistically significant
p-value	< .001	Relationship is significant
Standardised beta for ABISQ	0.241	Higher ABIS predicts higher SEBIS

It is an interesting finding, and it needs to be taken with a pinch of salt. It doesn't imply that impulsiveness helps substantively to create cybersecurity behaviours in practice. Students who were more impulsive also showed greater intentions to behave securely. Self-reported intention may not be congruent with actual behavior. But an impulsive student can have a clear vision of what behaviour is secure and he or she may also express firm plans in the survey. In any real world scenario, that same student, however, could still act quickly, ignore a warning or click on a suspicious link. This discrepancy is of major importance for the interpretation of the result.

The outcome can also be due to online training. Someone more impulsive might react to a security message, warning, or directive. After being inculcated with security concepts, this can create greater formal commitments. But these goals might not be secured if the training lacks repetition, practice and behaviour reinforcement. This is so because the result comes out to be a plus point and a challenge in the world of Online platforms. The advantage

of online training is that prompts, quizzes, scenarios, and immediate feedback can be utilized to draw attention to the training. But the difficulty is attention isn't always translated into secure behaviour. It is important that this is not limited to raising awareness, and should incorporate repeated decision based activities.

4.6.1 Attentional Impulsiveness

Attentional impulsiveness was analyzed in a sub-analysis. This resulted in a significant statistic; R squared = .068, $p < .001$. The coefficient was greater than 0. High levels of attentional impulsiveness were related to high security behaviour intentions. Again, this is not in the anticipated negative manner. It implies that although pupils may overestimate other pupils' need for secure behaviours, just because they experience impulsiveness in attention rather than persistent and excessive inattention they may still value such secure behaviour when asked about it using the structured questionnaire.

Table 13: Regression Result for Attentional Impulsiveness

Statistic	Value	Interpretation
R	0.261	Weak positive relationship
R squared	0.068	Explains 6.8% of variance
F statistic	34.877	Significant model
p-value	< .001	Statistically significant
Coefficient for Attention	0.211	Positive effect on SEBISQ

This finding should indicate an interaction between attentional impulsiveness and training material, the interaction of which is complex. Pupils with attention difficulties might realise that rules are important and remember to remind themselves. This is why they might feel more confident about their security intentions, as they understand that they are in a vulnerable position. This is not to be interpreted literally. The explanation value was low. This is a result that indicates that the researcher can measure the relationship to SEBISQ to attentional impulsiveness, however does not account for the significant variation in security intentions. Other factors are still important.

4.6.2 Non-Planning Impulsiveness

The dimension of non-planning impulsiveness was also looked at because planning and delayed judgment in making decisions is often necessary in cybersecurity. Students must take time to avoid clicking on links, use longer password, update devices, and possibly establish rules for data handling. If, on the other hand, there is a lack of planning, security behaviour intentions could be expected to be lower. Results indicated a statistically

significant relationship, but there was not a great deal of explanatory value for that relationship. This suggests that impulsiveness dimensions should not be considered as being equivalent. Security attitudes can be affected in a variety of ways by different aspects of impulsiveness.

If cybersecurity training will be offered online, then it may require pauses for practice and checkpoints for decision making, the finding argues. Perhaps a learning platform can be set up so that a learner hesitates before taking action as they are prone to acting out without planning. For instance, in simulated phishing tasks, students may need to recognize signs of a phishing scam prior to choosing a response. The types of password activities might include guiding students to compare weak and strong password selection. In scenario based exercises students might be given the opportunity to make choices about what to do with sensitive information. These features can be useful to transform the general sense of wanting to be more secure into more specific actions.

4.6.3 Interpretation of the Unexpected Direction

One of the most critical findings of this chapter is the unexpected positive connection between impulsiveness and intentions to protect participants' security. This helps to keep the conversation from being too broad. It reveals that behavioral characteristics and cybersecurity training do not always have a direct relationship. The initial research hypothesis was that impulsiveness would be negatively associated with security behaviour intentions. Findings indicated the contrary cases with regard to self-reported intentions. There is nothing wrong with this analysis. It reveals contradictions in students' behaviour. A student may not only be impulsive but also understand safe practices. It could happen when the intention is put to the test under pressure.

This outcome also illustrates that intention measures are not a good basis for inference. SEBIS assesses students' intentions. Doesn't see all real security decisions. This can be mitigated by using online platforms that can gather informative performance metrics via simulations and practical application. There is a need for self-report scales in future training, alongside behavioural tasks, to achieve the desired results. This would enable researchers to compare the students' planned and actual responses to real-world cyber risks.

4.7 Hypothesis 3: Behavioural Traits and Cyber Performance

The third hypothesis was that the intentions of engaging in security behaviour, impulsiveness and problematic Internet use would affect student cyber performance. When the raw performance score was examined as an individual variable, correlations were not statistically significant with either PIUQ, ABISQ or SEBISQ. Impliedly, the behavioural measures were low correlations with cyber performance in simple correlations. It is a balance to be interpreted here. But it shouldn't make people overlook the importance of behavioral attributes. It is important to note that Cyber performance in the training context might be influenced by a set of factors larger than the direct influences of the two variables listed above.

Table 14: Summary of Performance Relationships

Relationship	r	p-value	Conclusion
ScoreRaw and PIUQ	-0.021	0.703	No significant relationship
ScoreRaw and ABISQ	0.080	0.149	No significant relationship
ScoreRaw and SEBISQ	0.023	0.680	No significant relationship

The absence of significant direct relationships with performance is meaningful. It shows that knowing a student's PIU, ABIS, or SEBIS score does not necessarily allow the researcher to predict their raw training performance. One reason may be that online training scores are influenced by module design and assessment style. If assessments are simple or repeatable, students may achieve acceptable scores even if their real security behaviour is weak. Another reason may be that students with different behavioural profiles can still perform similarly on short online tasks. Cyber performance may therefore depend on knowledge, motivation, prior exposure, test format, and engagement level rather than on behavioural traits alone.

This result is important for the research question on the benefits and challenges of online platforms. A key benefit of platforms such as KnowBe4 and Brightspace is that they can record completion and performance data at scale. This creates evidence that universities can use to monitor training uptake. However, the challenge is that completion or score data may not fully represent secure behaviour. A student may pass a module but still fail to apply the learning in daily digital practice. This means that universities should use performance scores carefully. They are useful indicators, but they should not be treated as complete proof of behavioural change.

The H3 result also suggests that behavioural training should be integrated with practical learning tasks. If behavioural traits do not directly explain score outcomes, then training design may need to capture deeper forms of performance. This can include scenario responses, phishing simulations, password creation tasks, and longer term follow-up measures. The study therefore supports a shift from one-time awareness delivery to evidence-informed cybersecurity education. Online platforms can support this shift because they can track learner progress, repeat content, and deliver targeted exercises. Yet this requires careful design and evaluation.

4.7.1 Cohort and Subject Area Considerations

The research question also asked about the effect of subject area on engagement levels and completion rates. The available data allowed some comparison between computing and non-computing groups, but the result for SEBISQ was not statistically significant. This means that the dataset did not demonstrate a strong disciplinary difference in reported security intentions. The finding challenges a common assumption that computing students are automatically more security conscious. It also strengthens the case for whole-university cybersecurity education.

At the same time, the high level of unspecified faculty data limits the strength of conclusions about subject area. If future studies want to assess cohort effects more accurately, they need cleaner demographic recording. They should also distinguish between course subject, level of study, prior technical experience, and actual engagement with modules. These are not the same. A student from a non-computing course may have strong digital skills, while a computing student may still ignore basic security practices. The study therefore supports a more nuanced approach to cohort analysis.

4.8 Discussion of Findings

The findings of this study are consistent with recent work showing that student cybersecurity behaviour is shaped by more than exposure to training content. Taha, Ali and Abbas (2025) show that vulnerability behaviour can create obstacles in e-learning, while Rama, Marx and Smith (2025), Hasan, Sampa and Mahmud (2025), and Alzaidi (2025) indicate that awareness levels vary among university student groups. Bhandari (2025) also connects student awareness to legal and policy remedies. These studies support the

interpretation that PIU, impulsiveness and security intentions should be understood as part of a wider behavioural and institutional problem rather than as isolated student traits.

The results also fit with studies that emphasise the need for cyber hygiene and ongoing behavioural reinforcement. Ojala, Sipola and Saharinen (2025) identify training gaps and diverse learning pathways in education, while Kocsis, Shepherd and Segal (2025) show that cyber hygiene training can be used to improve student online behaviour. This supports the conclusion from Chapter 4 that a single online module may create awareness, but lasting secure behaviour requires repeated, targeted and evidence-based training.

The findings show that online cybersecurity training among students is shaped by both platform benefits and behavioural challenges. The strongest result was the negative relationship between problematic internet use and security behaviour intentions. This provides evidence that online cybersecurity training must address the human factor. Students who experience more problematic internet use may be less likely to report strong secure behaviour intentions. This matters because online platforms place responsibility on learners to engage, complete, and apply the training. Where self-regulation is weak, platform access alone may not be enough.

The impulsiveness findings were more unexpected. Instead of showing a negative relationship with security behaviour intentions, ABISQ showed a positive relationship. This result suggests that self-reported intentions may be shaped by awareness, perceived vulnerability, or response to survey prompts. It also shows that students can hold secure intentions while still being behaviourally vulnerable. This has practical importance. Online training should not assume that intention equals action. The training must create opportunities to practise secure decisions in realistic settings.

The performance findings were also cautious. Raw performance was not significantly related to the three behavioural scales in the correlation analysis. This suggests that cyber performance in online training may be influenced by factors not fully measured in this study. Module design, difficulty level, previous exposure, time on task, and student motivation may all matter. Therefore, universities should avoid using completion scores as the only measure of training effectiveness. A more robust evaluation would combine completion data, performance scores, behavioural simulations, and follow-up measures.

The findings support several benefits of online cybersecurity training. Online platforms can reach large student populations. They can provide consistent content across

cohorts. They can include modules on phishing, internet security, secure behaviour, scams, and acceptable use. They also allow institutions to collect data on engagement and performance. These benefits are important in a university setting where students come from different disciplines and levels of study. The Bournemouth University case shows that a platform approach can make cybersecurity training more scalable than face-to-face delivery alone.

The findings also reveal several challenges. Voluntary participation may reduce completion and create selection bias. Students who are already more interested in cybersecurity may be more likely to engage. Missing demographic data can weaken analysis. Self-reported measures can show intentions but may not capture actual behaviour. Differences between behavioural traits and performance outcomes can also make evaluation difficult. These challenges do not undermine online cybersecurity training. They show that online platforms need stronger design, clearer data capture, and more behaviour-focused evaluation.

Overall, the results answer the research aim by showing that student performance and engagement with online cybersecurity learning are influenced by behavioural traits, but not in a simple or uniform way. PIU was clearly associated with weaker security behaviour intentions. Impulsiveness had a more complex positive association with self-reported intentions. Cyber performance was not directly explained by the behavioural scales. These findings support a practical conclusion. Online cybersecurity training is valuable, but it should be designed as a behaviour change intervention rather than only as an information delivery tool.

Table 15: Hypothesis Summary

Hypothesis	Result	Interpretation
H1	Supported	Higher PIU was linked to lower security behaviour intentions
H2	Not supported in expected direction	Impulsiveness had a positive relationship with reported security intentions
H3	Partially supported	Behavioural traits related to intentions, but not directly to raw performance

5 DESIGN

5.1 Introduction

The statistical results are used to inform design considerations for this chapter. It's there because the study itself does not lie solely with the presentation of the results. The findings should feed into the learning of the methods and ways that online cyber security trainings can be enhanced to enhance students. Although there are benefits in being able to reach a large number of people with online training, it is found to be useful only if the training is repeated, relevant and linked with real choices made by the users (Bada, Sasse and Nurse, 2019; Sharma and Rathi, 2021). The design implications are thus on inclusivity of access, behavioral reflection, scenario-based assessments, and data-driven improvements.

In the Bournemouth University case, they did find that a training platform could deliver consistent service and stats that can be useful. At the same time, it illustrates that the current learning behaviour of the learner is important. There was a negative association between problematic internet use and security behaviours intentions. The impulsiveness behaviour did not go as expected, implying that there may be a difference between intention and practice. The results indicated that the model of design in the future training should be freed from the module and quiz approach. It should relate to students' activities and their discipline/field of studies.

5.2 Design Implications for Online Cybersecurity Training

There are some recent studies on learning design that provide support for the proposed cybersecurity training design. The potentials of the cyber range for all education levels are illustrated by Lazarov et al., (2025) and how the multimodal and adaptive gamification approach can be applied to cybersecurity competence training is highlighted by Albaladejo-Gonzalez et al., (2025). Other authors address requirements and challenges in remote cybersecurity laboratories (Otoum et al., 2025) as well as, environment management platforms with experiential cybersecurity education (Arnold, Ford and Saniie, 2025). The practical and accessibility aspects of combining accessible and adaptive content with technical support have been supported in these studies and led to the design implication that such a university platform should integrate accessibility combined with practical activities; adaptive content and clear technical support.

Future use of intelligent tutoring and applied support needs to be taken into account as well. In the case of graduate cybersecurity programmes, Mukherjee, Le and Chow (2025) note that AI-powered intelligent tutoring systems can be beneficial and are collaborating with this. Nelson, Doupe and Shoshitaishvili (2025) look at how that can be used for AI as applied

cybersecurity tutors. Similarly, Narain et al. (2025) suggest a practical course model following experiential learning theory (ELT). Next generation online cybersecurity training might incorporate aspects of both automated and scenario-based tasks, yet it is important that these systems are created carefully to ensure that students will still internalize correct judgement and security practices.

The first design implication associated with the first rule of cybersecurity is that cybersecurity should be taught nationwide within universities. There was no significant difference between the computing and non-computing group in their security behaviour intentions in the analysis conducted. This stands as evidence that one shouldn't take the place of training by relying on technical points. Email, cloud systems, virtual learning environments and accounts are utilised by all students. This entails providing the same set of security awareness on a common shields for all students (Center for Internet Security, 2021; Wiechetek and Medrek, 2022).

The second design implication is that training must contain actually the behavioral reflection and self-reflection. That a significant negative correlation has been found for PIU and SEBIS means that the students who have more problematic patterns of internet use may have less security intentions. Something useful to design a training should be allowing students to consider the following behaviours: Re-using passwords, clicking on suspicious links, unprotected browsing and ignoring warnings. This is similar to Caplan (2010), Hadlington (2017), Sussman and Leavitt (2023), where they found that self-regulation and risk perception are related to secure or risky behaviour, respectively, and Egelman and Peer (2015), where they found that secure behaviour is related to self-regulation and risk perception is related to insecure behaviour and also with the studies carried out by Bada et al., (2019) who found that self-regulation positively related to the acquisition of secure behavior, while the perception of risk was related to the acquisition of risky behavior.

5.3 Proposed Training Design

An inclusive design across student groups will also be required for the proposed design. Collaborative online international learning has proven to enhance cybersecurity awareness, as demonstrated by Lui, Womack and Orton (2025), and the use of Internet of Things (IoT) has been investigated for increasing the participation of heterogeneous audiences in cybersecurity education by Namukasa et al. (2025). Serik et al. (2025) point to the importance of embedding Cyber Security into teacher training and Fukuda (2025) demonstrates how to tailor cyber range training to IT industry stakeholders other than IT. The following studies are supportive of this design, that is, it doesn't assume that all students are

computing specialists. It should present the severe learning points for non-technical learners, and also offer high-level practice for technical learners.

The needs of the participants would first be diagnosed and short training program hypothesized in a suitable training design. Never would be used to label individual students this stage. It would be used to identify the patterns of intentions of security behaviour in the group, problematic Internet use and confidence. In stage 2, a brief core module would be given via Brightspace or other platform. The main module should include phishing, password security, scams, safe Internet browsing and acceptable use. At the third stage of the Government's rule of law implementation, examples of subjects should be used. A study of customer data fraud could be undertaken by business students. Health students had the option to explore the aspect of confidentiality in relation to patient data. Students in the computer field could explore incident response and configuring systems for protection.

The fourth should be in scenario form. Pupils need to recognise suspicious messages, make safe responses to incidences of account compromise, and what to do if the device is lost. Microlearning reminders throughout the academic year – fifth stage. The likelihood of short reminders being more sustainable than the long one-off modules is greater. If there's a change in threat patterns, this design will enable upgrading on the training side (Wang and Chen, 2020; Hall, 2021).

Table 16: Design principles for student cybersecurity training

Design principle	**Reason from findings**	**Practical response**
Inclusive baseline	Computing status did not guarantee stronger intentions	Train all students
Behavioural reflection	PIU weakened security intentions	Add habit-based reflection
Scenario assessment	Raw scores did not predict behaviour	Use phishing and response scenarios
Microlearning	Cyber behaviour needs reinforcement	Repeat short modules
Data quality	Faculty data were incomplete	Improve cohort recording

5.4 Design Summary

The future design puts the issue of online cybersecurity courses as a behavioral and educational intervention. Preserves and retains many of the good features of online platforms such as scale, consistency and tracking. It also responds to the identified areas of weaknesses such as the restrictions on raw scores and the relevance of students' behaviour. This design is also highly pertinent to Bournemouth University – the current Brightspace and KnowBe4

account for a viable delivery model already exists. The biggest change is to increase the aspect of reflection, repetition and practice in the training.

6 EVALUATIONS

6.1 Introduction

Based on this study, this chapter discusses the online cybersecurity training approach. There is a need for evaluation as training should not be measured purely by accessibility of students. Its effectiveness should be considered in terms of its ability to get it to the intended audience, effective engagement, enabling positive intentions and creating deliverables that the university can use. The evaluation is based on the findings of Chapter 4 as well as cybersecurity awareness research by Alasmary et al. (2020), Bada et al. (2019) and Tavakol and Dennick, (2011).

6.2 Evaluation of Benefits

Current research on online education and cyber security resources are used to support the evaluation of benefits. Chidinma and Idemudia (2025) review cybersecurity issues pertaining to an open and distance learning system and Sadiqzade and Alisoy (2025) present risks and solutions to online learning. In other research, Mca and Balasirisha (2025) showed additional cybersecurity awareness case studies for online education. These studies validate the assessment that the internet can offer access to training consistently accessible, however it relies upon the degree of integration of the protection material in the learning programs.

The security and privacy of student data also rely on safeguarding these in educational technologies. Creating security guarantees for student data in E-Learning technologies is a complex issue, as highlighted by Patience, Innocent and Jigiedous (2025). Against the background of digital educational technologies use in higher education systems, Parfonova and Zinchenko (2025) present the problem of countering cyber threats in higher education. The results of these studies validate the notion of the double role played by online cybersecurity training. It helps students to form good habits, while educating universities about the security and good governance of the learning platforms they utilize.

First benefit is that it is scalable. Bournemouth University had the opportunity to provide training to a wide number of students via the online platform. It would be hard to get to that degree of knowledge in class in just one hour. The second advantage is that it's consistent. Online modules can be provided to all learners to ensure they are provided with the same core information on phishing, scams, password security and acceptable use. The third advantage of an exchange-traded fund is that it is flexible. The trainees/edumnents can take the training in their own study time. Online platforms are an appealing alternative to large universities' (Al-Bakri et al., 2020; Wang and Chen, 2020; NCSC, 2020; Jisc, 2020) benefits.

6.3 Evaluation of Challenges

These challenges, like those identified in this study, are representative of the broader literature. Salem, Samara and Al-Tamimi (2024) highlight the challenges to attaining a uniform curriculum in cybersecurity education on the Internet, and Tazi, Shrestha and Das (2023) demonstrate that online education can raise issues regarding support, privacy and safety. Furthermore, as demounted in Otoum et al. (2025), the software requirement, access and reliability of the remote laboratories, can influence the students experience; which underlines the need to carefully plan for them. These studies help to substantiate the findings that online cybersecurity training isn't always effective. It requires good design, sound systems, and access to resources and sound institutional controls.

The key problem is engagement! Pursuing voluntary training could bring in students that are already more motivated in the area of cyber security. May not reach certain students who require the most support. This has a real-life issue for institutions as simply having an online module does not demonstrate that the risk has been tackled. The second problem is one of assessment 'validity'. Results indicated that raw performances were not significantly related to the primary measures of behaviours. So, a precaution must be taken while interpreting the results of the quiz (Moustafa et al., 2021; Yin, 2014; Mishra and Alok, 2022).

Table 17: Evaluation criteria for online cybersecurity training

Criterion	**Evidence needed**	**Purpose**
Reach	Number and proportion of students accessing training	Shows coverage
Engagement	Completion, time spent and repeat activity	Shows participation depth
Learning	Knowledge and scenario scores	Shows understanding
Behaviour	Observed choices in simulations	Shows transfer
Sustainability	Updates and repeat refreshers	Shows long-term value

6.4 Evaluation Summary

Based on the evaluation, cybersecurity training online is an excellent way to deliver training but cannot stand alone. It is best combined with behavioural design and/or with practical assessment and frequent review. Bournemouth University demonstrates how useful online platforms can be in enabling the collection of useful evidence at an institutional level. It also verifies that there needs to be a careful analysis of that evidence. There should be an enhanced evaluation model that incorporates elements of reach, engagement, learning, behaviour and sustainability.

7 RECOMMENDATIONS

7.1 Recommendations for Practice

The exercise suggestions are based on research highlighting learning strategies and behaviourally reinforcing the instruction. Sarita et al. (2025) have identified the need for adequate learning strategies for cybersecurity awareness of students and what Roopa et al. (2025) illustrate is the use of gamified learning platform to support cyber learning. However, Kocsis, Shepherd and Segal (2025) demonstrate that structured cyber hygiene instruction has a possible impact on students' online actions. Examples of these sources include the recommendation that Bournemouth University integrate awareness content with short, gradual practice exercises with reminders and reflection on the behavioural content with a focus of additional one-off module completion.

One recommendation is for students to all receive cybersecurity training. The results do not substantiate the thesis of automatic improvement of security intentions of students, since there is no significant difference between the two sample groups. A core concept then should be established for all learners when they enter a school. The second suggestion is for employees to have some form of behavioural self-reflection during trainings. Pupils are to reflect on their own online behaviours and how this might potentially raise cyber risk (Caplan (2010); Hadlington (2017).

Table 18: Practical recommendations

Recommendation	**Purpose**	**Expected benefit**
Train all students	Avoid discipline-based assumptions	Improves baseline awareness
Add behavioural reflection	Connect content to habits	Improves relevance
Use scenarios	Assess applied judgement	Improves validity
Repeat microlearning	Reinforce cyber behaviour	Supports retention
Improve data quality	Record cohort details accurately	Improves evaluation

7.2 Recommendations for Policy

The study of legal remedies and data protection and digital education governance, which bolsters the policy recommendations, will also be identified. Bhandari (2025) calls for the need of support through policies where cybersecurity awareness education for students is concerned and Patience, Innocent and Jigiedous (2025) stress on protecting student data in EdTech tools. Furthermore, Parfonova and Zinchenko (2025) illustrate that the education sector has a need for strategy to defend itself against cyber threat in digital learning environment at higher education systems. These sources argue for a policy context in which

cybersecurity education is an integral component of students' digital literacy and institutional risk management and platform governance.

Cybersecurity should be included in the digital literacy of students and be included in the university guidelines. It should not be a nice to have item that is regarded as a compliance activity. A competence-based requirement would help ensure the institutional's resilience, and also contribute to the employability of the students. Policy needs to also outline the process of training data collection, protection and utilization. This is significant as behavioural data is sensitive and needs to be reported as an aggregate (Jones and Simon, 2019; Jisc, 2020).

7.3 Recommendations for Future Research

Future studies will investigate effectiveness with models that go beyond simple awareness training and provide adaptation and/or AI assistance. Albaladejo-Gonzalez et al. (2025), Mukherjee, Le and Chow (2025), Nelson, Doupe and Shoshitaishvili (2025) and Narain et al. (2025) present several such new developments in the field of cybersecurity education: gamified systems, intelligent tutors and experiential courses. In future studies, it is important to compare to see which type of design will increase the level of security intent and behavior, adaptive simulations against standard online modules; applied browser environments against tutor supported tasks.

Further studies need to be done which involve more than 1 university. A multi-case study would help to establish if the Bournemouth University research is applicable in other institutional settings. A need for future research is also for the use of longitudinal data. This would help to demonstrate student retention of cyber awareness knowledge and whether over time repeated microlearning would have a positive effect on behaviours (Yin, 2014; Snyder, 2019).

Table 19: Study limitations and future responses

Limitation	**Effect**	**Future response**
Single case study	Limits wider generalisation	Use multi-case research
Secondary data	Limits control over variables	Plan future data collection prospectively
Self-report scales	May not capture actual behaviour	Add observed behavioural tests
Voluntary participation	Creates possible self-selection bias	Compare completers and non-completers
Raw performance score	May not show applied competence	Use scenario and simulation measures

8 CONCLUSIONS

In overall, the thesis is consistent with recent research and literature indicating that online cybersecurity education is most effective if being scalable, practical, inclusive and behaviour focused. All the above authors (Ahmed et al., 2024; Salem, Samara and Al-Tamimi, 2024; Vykopal et al., 2023; Erendor and Yildirim, 2022; Lazarov et al., 2025) attest to the idea that online delivery may facilitate increased cybersecurity training availability. The collective evidence, however, indicates that alone platform access is not sufficient, either. Pupils require a safe structure, practice, protection on data sharing and frequent reinforcement of cyber hygiene. The Bournemouth case thus adds to the broader literature as it demonstrates the (need for a combination of behavioural characteristics and platform design to be taken into account when designing a cybersecurity training for students.

This thesis explored the difficulties and potential of online training tools in the field of cybersecurity training with students. It is using the Bournemouth University's KnowBe4 pilot as the quantitative single case study. The study revealed that there are clear advantages with online platforms such as scalability, consistency, flexibility, and data generation. The advantages of these are useful for universities which face the necessity of raising cyber awareness among various students (Al-Bakri et al., 2020; NCSC, 2020).

The study also revealed that a number of critical issues for online channels. DO NOT assume Engagement. It does not necessarily follow that behaviors will change when they are completed. Raw results of the tests may not indicate actual security skills. An association with lower security behaviour intentions was significantly related to problematic internet use. It may be concluded that self-reported intention must be interpreted with caution, because there was an unexpected positive relationship between impulsiveness and report intentions about the security measure. This finding aligns with previous result about the impact of impulsiveness on self-reported intentions to step up toward the security measures (Egelman and Peer, 2015; Moustafa et al., 2021).

The primary finding is that an online cybersecurity educational and behavioural intervention is needed. It should NOT be just for technical students. It should require the participation of all students, and rely on real scenarios, will prompt reflection on online behaviours and will assess applied judgement. Through the Bournemouth University case, it has been illustrated how online cybersecurity courses can contribute to the institutional resiliency, but only if they are designed, assessed and improved. Length of the main body around 15,000 words.

REFERENCES

Abdiraman, A., Aldasheva, L., Darmenov, B., Omurzakov, T.I. and Zakirova, A.B. (2023) Comparative analysis of application platform for learning cybersecurity through the capturing the flag competitions. Bulletin of L. N. Gumilyov Eurasian National University Technical Science and Technology Series. Available at: https://doi.org/10.32523/2616-7263-2023-145-4-49-57.

Ahmed, A., Watterson, C.A., Alhashmi, S. and Gaber, T. (2024) How universities teach cybersecurity courses online: A systematic literature review. Frontiers in Computer Science, 6. Available at: https://doi.org/10.3389/fcomp.2024.1499490.

Aivazpour, Z. and Rao, H.R. (2022) Impulsivity and online risk behaviour in security contexts. Information and Computer Security, 30(4), pp.521-538.

Al-Bakri, A., Elrehail, H. and Alzoubi, H. (2020) Online learning and cybersecurity awareness in higher education. Education and Information Technologies, 25(6), pp.4725-4741.

Al-Fatlawi, H.H.M.A. (2024) Awareness of cyber security aspects in distance education. Journal of Pedagogical Sociology and Psychology. Available at: https://doi.org/10.33902/jpsp.202424403.

Al-Sherideh, A., Maabreh, K., Maabreh, M., Al Mousa, M.R. and Asassfeh, M. (2023) Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study. International Journal of Advanced Computer Science and Applications. Available at: https://doi.org/10.14569/ijacsa.2023.0140516.

Alasmary, W. and Alhaidari, F. (2020) Cybersecurity awareness and training in online learning environments. International Journal of Advanced Computer Science and Applications, 11(12), pp.1-8.

Albaladejo-Gonzalez, M., Nespoli, P., Gomez Marmol, F. and Ruiperez-Valiente, J.A. (2025) A multimodal and adaptive gamified system to improve cybersecurity competence training. Cluster Computing, 28. Available at: https://doi.org/10.1007/s10586-025-05264-6.

Alharahsheh, H.H. and Pius, A. (2020) A review of key paradigms: positivism versus interpretivism. Global Academic Journal of Humanities and Social Sciences, 2(3), pp.39-43.

Alzaidi, N. (2025) Cybersecurity awareness among female students at Taif University's faculty of computing and information technology. Global Journal of Information Technology: Emerging Technologies. Available at: https://doi.org/10.18844/gjit.v15i1.9722.

Armas, J. and Taherdoost, H. (2025) Cybersecurity-aware culture in higher education institutions. Journal of Cybersecurity Education, 8(1), pp.15-32.

Arnold, D., Ford, J. and Saniie, J. (2025) Architecture of an efficient environment management platform for experiential cybersecurity education. Information. Available at: https://doi.org/10.3390/info16070604.

Bada, M., Sasse, A.M. and Nurse, J.R.C. (2019) Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv, pp.1-14.

Barbu, M., Zamfiroiu, A., Marinescu, I.A., Iordache, D.-D. and Bumbac, R. (2023) Empowering digital education: Understanding students' perceptions about risks and threats in the shifting educational paradigm. Studies in Informatics and Control. Available at: https://doi.org/10.24846/v32i4y202310.

Bhandari, B. (2025) Cybersecurity awareness amongst university students: Legal remedies and policies to mitigate risks. Unity Journal. Available at: https://doi.org/10.3126/unityj.v6i1.75557.

Caplan, S.E. (2010) Theory and measurement of generalized problematic internet use. Computers in Human Behavior, 26(5), pp.1089-1097.

Center for Internet Security (2021) Cyber hygiene guide. East Greenbush: CIS.

Chidinma, A.E. and Idemudia, A.J.-H. (2025) Evaluating the effectiveness of cybersecurity measures in safeguarding online educational resources: A case study of the University of Port Harcourt Open and Distance Learning System. Journal of Advances in Education and Philosophy. Available at: https://doi.org/10.36348/jaep.2025.v09i07.003.

Christensen, M., Britze, D., Vejlin, J., Sorensen, L. and Pedersen, J. (2023) The Privacy Universe: A game-based learning platform for data protection, privacy and ethics. 2023 IEEE Global Engineering Education Conference, pp.1-8. Available at: https://doi.org/10.1109/educon54358.2023.10125160.

Coutlee, C.G., Politzer, C.S., Hoyle, R.H. and Huettel, S.A. (2014) An abbreviated impulsiveness scale constructed through confirmatory factor analysis. Frontiers in Psychology, 5, pp.1-12.

Demetrovics, Z., Szeredi, B. and Rozsa, S. (2016) The three-factor model of internet addiction. Behavior Research Methods, 40(2), pp.563-574.

Egelman, S. and Peer, E. (2015) Scaling the security wall: Developing a security behavior intentions scale. Proceedings of the CHI Conference on Human Factors in Computing Systems, pp.2873-2882.

Erendor, M.E. and Yildirim, M. (2022) Cybersecurity awareness in online education: A case study analysis. IEEE Access. Available at: https://doi.org/10.1109/access.2022.3171829.

Fukuda, T. (2025) Bridging the cybersecurity divide: A reskilling initiative for non-IT professionals through adapted cyber range training. WSEAS Transactions on Advances in Engineering Education. Available at: https://doi.org/10.37394/232010.2025.22.7.

Hadlington, L. (2017) Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity and risky cybersecurity behaviours. Heliyon, 3(7), pp.1-18.

Hall, J. (2021) Gamified learning and cybersecurity training outcomes. Journal of Cyber Education, 6(1), pp.55-72.

Hasan, M., Sampa, M.A. and Mahmud, M.K. (2025) Understanding cybersecurity awareness among students in Bangladesh. Society & Sustainability. Available at: https://doi.org/10.38157/ss.v7i1.682.

Hnaif, A., Derbas, A.M. and Almanasra, S. (2024) Cybersecurity integration in distance learning: An analysis of student awareness and attitudes. Indonesian Journal of Electrical Engineering and Computer Science. Available at: https://doi.org/10.11591/ijeecs.v33.i2.pp1057-1066.

Hu, Y. (2022) Providing a hands-on advanced persistent threat learning experience through ethical hacking labs. Journal of The Colloquium for Information Systems Security Education. Available at: https://doi.org/10.53735/cisse.v9i1.153.

Jisc (2020) Cyber security in higher education. Bristol: Jisc.

Jones, R. and Simon, L. (2019) Data protection compliance and higher education. Information Compliance Journal, 12(3), pp.21-34.

Junior, A.O., Funchal, G., Queiroz, J., Loureiro, J., Pedrosa, T., Parra, J. and Leitao, P. (2022) Learning cybersecurity in IoT-based applications through a capture the flag competition. 2022 IEEE 20th International Conference on Industrial Informatics, pp.560-565. Available at: https://doi.org/10.1109/indin51773.2022.9976079.

Karagiannis, S., Magkos, E., Chalavazis, G. and Nikiforos, M.N. (2022) Analysis and evaluation of capture the flag challenges in secure mobile application development. International Journal on Integrating Technology in Education. Available at: https://doi.org/10.5121/ijite.2022.11202.

Kocsis, D., Shepherd, M. and Segal, D. (2025) Teaching tip cyber hygiene training: Using a Salesforce developer module to improve student online behaviors. Journal of Information Systems Education. Available at: https://doi.org/10.62273/cueu6233.

Lazarov, W., Schafeitel-Tahtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P. and Fujdiak, R. (2025) Lessons learned from using cyber range to teach cybersecurity at different levels of education. Technology, Knowledge and Learning. Available at: https://doi.org/10.1007/s10758-025-09840-y.

Lui, A.T., Womack, C. and Orton, P. (2025) Collaborative online international learning as a third space to improve students' awareness of cybersecurity. Education and Information Technologies, 30, pp.13835-13856. Available at: https://doi.org/10.1007/s10639-025-13336-8.

Mca, K. and Balasirisha, K. (2025) Cybersecurity awareness in online education: A case study analysis. International Journal of Research Publication and Reviews. Available at: https://doi.org/10.55248/gengpi.6.0525.1921.

Mishra, S.B. and Alok, S. (2022) Handbook of research methodology. New Delhi: Educreation Publishing.

Moustafa, A.A., Bello, A. and Maurushat, A. (2021) The role of user behaviour in improving cybersecurity performance. Behaviour and Information Technology, 40(9), pp.1-14.

Mukherjee, M., Le, J. and Chow, Y.-W. (2025) Generative AI-enhanced intelligent tutoring system for graduate cybersecurity programs. Future Internet, 17, p.154. Available at: https://doi.org/10.3390/fi17040154.

Namukasa, M., Chauhan, B.B., Swords, C., Gough, C., Dymanus, W., Diresta, C., Vitali, J., Sharma, V., OConnor, T.J. and Carroll, M. (2025) Diversifying cybersecurity: Evaluation of an Internet of Things (IoT)-based cybersecurity training course designed to bridge the diversity gap. Journal of Cybersecurity Education, Research and Practice. Available at: https://doi.org/10.62915/2472-2707.1232.

Narain, S., Rayavaram, P., Morales-Gonzalez, C., Harper, M., Abbasalizadeh, M., Vellamchety, K. and Fu, X. (2025) Practical cybersecurity education: A course model using experiential learning theory. Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1. Available at: https://doi.org/10.1145/3641554.3701922.

NCSC (2020) Cyber threat to universities. London: National Cyber Security Centre.

Nelson, C. and Shoshitaishvili, Y. (2024) DOJO: Applied cybersecurity education in the browser. Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1. Available at: https://doi.org/10.1145/3626252.3630836.

Nelson, C., Doupe, A. and Shoshitaishvili, Y. (2025) SENSAI: Large language models as applied cybersecurity tutors. Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1. Available at: https://doi.org/10.1145/3641554.3701801.

Ojala, A.-L., Sipola, T. and Saharinen, K. (2025) Cybersecurity awareness and hygiene development in Finnish vocational education: Staff perceptions, training gaps and diverse learning pathways. Information & Computer Security. Available at: https://doi.org/10.1108/ics-12-2024-0311.

Otoum, N.A., Al Maqousi, A., Alauthman, M. and Almomani, A. (2025) Remote labs in cybersecurity education: Analyzing software requirements and challenges. International Journal of Cloud Applications and Computing, 15, pp.1-27. Available at: https://doi.org/10.4018/ijcac.383300.

Paculanan, R.S., Tadeo, R.L., Caliliw, M.T., Atal, C.P. and Sadol, J.N. (2024) Cyberverse: A game-based learning application for cyber security. International Journal of Latest Technology in Engineering Management & Applied Science. Available at: https://doi.org/10.51583/ijltemas.2024.131001.

Parfonova, I. and Zinchenko, O. (2025) Countering cyber threats in the context of digital educational technologies in the higher education system of Ukraine. Scientific Journal of Polonia University. Available at: https://doi.org/10.23856/6729.

Patience, B.A., Innocent, O.S. and Jigiedous, O.F. (2025) Enhancing security and privacy in EdTech tools: Safeguarding student data in the digital learning era. Journal of Science Innovation and Technology Research. Available at: https://doi.org/10.70382/ajsitr.v9i9.041.

Prada, M.A., Fuertes, J.J., Rodriguez-Ossorio, J., Gonzalez-Herbon, R., Gonzalez-Mateos, G. and Dominguez, M. (2023) Hands-on training in industrial cybersecurity for a multidisciplinary master's degree. IFAC-PapersOnLine. Available at: https://doi.org/10.1016/j.ifacol.2023.10.850.

Raju, R., Hidayah, N., Rahman, A. and Ahmad, A. (2022) Cyber security awareness in using digital platforms among students in a higher learning institution. Asian Journal of University Education. Available at: https://doi.org/10.24191/ajue.v18i3.18967.

Rama, P., Marx, B. and Smith, R. (2025) Cybersecurity awareness among accounting students at a South African public university. South African Journal of Information Management. Available at: https://doi.org/10.4102/sajim.v27i1.1948.

Roopa, V., Swethaa, S., Sandhiyab, S. and Priyamvadha, P.G. (2025) Cyber learning gamification platform. International Journal of Research Publication and Reviews. Available at: https://doi.org/10.55248/gengpi.6.0525.1981.

Sadiqzade, Z. and Alisoy, H. (2025) Cybersecurity and online education: Risks and solutions. Luminis Applied Science and Engineering. Available at: https://doi.org/10.69760/lumin.20250001001.

Saeed, S. (2023) Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. Sustainability. Available at: https://doi.org/10.3390/su15129426.

Salem, M., Samara, K. and Al-Tamimi, A.-K. (2024) Navigating challenges in online cybersecurity education: Insights from postgraduate students and prospects for a standardized framework. ACM Transactions on Computing Education, 24, pp.1-32. Available at: https://doi.org/10.1145/3703163.

Salem, M.A. and Sobaih, A. (2023) A quadruple E approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in Saudi Arabia amid COVID-19 pandemic. Electronics. Available at: https://doi.org/10.3390/electronics12102268.

Sarita, K., Kashish, Singh, P., Singh, G. and Kaur, S. (2025) Learning strategies for promoting cybersecurity awareness among students: A brief review. International Journal for Multidisciplinary Research. Available at: https://doi.org/10.36948/ijfmr.2025.v07i03.44564.

Serik, M., Tleumagambetova, D., Tutkyshbayeva, S. and Zakirova, A. (2025) Integration of cybersecurity into computer science teachers' training: A systematic review. International Journal of Engineering Pedagogy, 15, pp.57-75. Available at: https://doi.org/10.3991/ijep.v15i4.53127.

Sharma, R. and Rathi, S. (2021) Online platforms for cybersecurity awareness and training. International Journal of Information Security Education, 7(2), pp.66-81.

Sussman, S. and Leavitt, A. (2023) Behavioural traits and technology use in online learning. Journal of Behavioral Addictions, 12(2), pp.210-224.

Svabensky, V., Vykopal, J., Horak, M., Hofbauer, M. and Celeda, P. (2024) From paper to platform: Evolution of a novel learning environment for tabletop exercises. Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1. Available at: https://doi.org/10.1145/3649217.3653639.

Swartz, S. and Nayak, D. (2024) Addressing the need for interculturality in cybersecurity education. Journal of The Colloquium for Information Systems Security Education. Available at: https://doi.org/10.53735/cisse.v11i1.176.

Taha, I.M., Ali, R.H.A. and Abbas, A.A. (2025) The impact of students' cybersecurity vulnerability behavior on e-learning obstacles. Organizacija, 58, pp.85-104. Available at: https://doi.org/10.2478/orga-2025-0006.

Tavakol, M. and Dennick, R. (2011) Making sense of Cronbach's alpha. International Journal of Medical Education, 2, pp.53-55.

Tay, A., Hayes, S.M., Wilson, D., Hall, E. and Kaufman, D. (2024) Gamified cybersecurity education through the lens of the information search process: An exploratory study of capture-the-flag competitions. Issues in Informing Science and Information Technology. Available at: https://doi.org/10.28945/5313.

Tazi, F., Shrestha, S. and Das, S. (2023) Cybersecurity, safety, and privacy concerns of student support structure for information and communication technologies in online education. Proceedings of the ACM on Human-Computer Interaction, 7, pp.1-40. Available at: https://doi.org/10.1145/3610055.

Verma, V. and Pawar, J. (2024) Assessment of students cybersecurity awareness and strategies to safeguard against cyber threats. Journal of Advanced Zoology. Available at: https://doi.org/10.53555/jaz.v45is4.4156.

Vykopal, J., Seda, P., Svabensky, V. and Celeda, P. (2023) Smart environment for adaptive learning of cybersecurity skills. IEEE Transactions on Learning Technologies, 16, pp.443-456. Available at: https://doi.org/10.1109/tlt.2022.3216345.

Wang, Y. and Chen, N. (2020) Online learning analytics and cybersecurity education. Computers and Education, 148, pp.1-11.

Weitl-Harms, S., Spanier, A.M., Hastings, J.D. and Rokusek, M. (2023) Framing gamification in undergraduate cybersecurity education. Journal of The Colloquium for Information Systems Security Education. Available at: https://doi.org/10.53735/cisse.v10i1.161.

Wiechetek, L. and Medrek, M. (2022) Non-technical students and cybersecurity awareness in higher education. Education Sciences, 12(9), pp.1-16.

Yin, R.K. (2014) Case study research: Design and methods. 5th edn. Thousand Oaks: Sage.

APPENDICES

Appendix A: Project Proposal Summary

The project investigated the challenges and benefits of using online platforms for cybersecurity training among students. The proposal identified online cybersecurity awareness, student engagement and behavioural traits as the central areas of inquiry.

Appendix B: Ethics Approval Summary

The original pilot study received ethical approval ID (65423) before data collection began. The present thesis used secondary anonymised data and did not involve new participants.

Appendix C: Dataset and Analysis Plan

Table C1: Dataset and analysis plan

Data element	**Planned use**
PIUQ	Measure problematic internet use
ABISQ	Measure impulsiveness
SEBISQ	Measure security behaviour intentions
ScoreRaw	Measure cyber training performance
Demographic data	Describe sample and compare groups

Appendix D: Cybersecurity Training Modules

Table D1: Cybersecurity training modules

Module	**Training theme**
1	Internet security
2	Security awareness
3	Secure online behaviour
4	Security culture
5	Phishing
6	Online scamming
7	Acceptable use of technology