Title Page

Title: Examining the efficacy of cybersecurity awareness in mitigating phishing when implementing e-learning in Secondary schools in Hong Kong.

Research question: To what extent can cybersecurity awareness empower secondary school students to mitigate phishing attempts during e-learning?

Jonathan Callaghan
Student ID: 12686209
University of Essex Dissertation Research Project
CYSPROJ_PCOM7E May 2023

Word count: 14269

Declaration

I declare that this thesis has been composed solely by myself and has not been submitted in any previous application for a degree in whole or in part. The work presented is entirely my own except where stated otherwise by reference or acknowledgement.

Abstract

Integrating e-learning in secondary schools has become an essential aspect of contemporary education, particularly in Hong Kong. The research project explores the implications of e-learning, focusing on the phishing cyber threat and its impact on students and educational institutions. The research used a mixed-method approach examining e-learning adoption by schools, assessing students' cyber awareness and analysing measures to mitigate phishing attempts. Participating students undertook questionnaires and a phishing simulation to assess their performance in managing the challenges of phishing emails aimed at schools. The findings suggest a distinct divide between students' cyber awareness and technical proficiency, emphasising educational institutions' vulnerability to cyber threats. Whilst technical proficiency and safeguarding are critical measures for educational leaders to implement, comprehensive cybersecurity education and training are necessary for all stakeholders. The research project offers the opportunity for students to assess their knowledge of phishing in a practical but controlled environment. The research underscores recommendations that to foster proficient and digital citizens, enhanced cyber awareness training, practical application of theoretical knowledge, and adoption of security technologies are required. This study highlights the risks associated with phishing and the challenges faced in Hong Kong and offers effective strategies to support a digitally secure society.

Acknowledgements

I would like to express my deepest gratitude to my supervisors, Dr. Samuel Danso and Dr. Cathryn Peoples, for their insightful guidance and continuous support through this research project. I am very thankful for the feedback and encouragement offered throughout this process, which provided excellent support throughout the stages of the project. I would also like to thank the Principal, students and staff at the Hong Kong Secondary School who allowed the research to occur and participated in the project. Finally, I would like to thank my family, who provided emotional support, encouragement, and understanding while I undertook the project.

Contents

List of tables and figures

1.0 Introduction (679 words)

From 20 January 2020 to 30 May 2023, Hong Kong's COVID-19 response was unique in its strategy to manage the virus. Schools were ill-prepared for the rapid shift in methodology to deliver curriculums to students online due to the suspension of the regular school day (Cheung, 2023). Students and staff were expected to stay home, and lessons would be delivered remotely; the connection between technology integration and teacher professional development was not fully established, and remote teaching was brought about due to parental pressure (Cheung, 2023).

During this period, teachers were subjected to disruption and cyber attacks, particularly phishing attempts. Teaching staff could be emailed false website links or receive non-genuine emails posing as Principals (Steed, 2023), and the insider threat was ever present, as disgruntled students attempted Zoom bombing, requesting teachers to impose as genuine users to disrupt lessons. The writer of this report received first-hand experience of such events that altered school policy, so all educators had to change privacy and security settings required for greater stringency so external malicious users did not disrupt lessons and infiltrate school networks. Many faculty staff found this implementation challenging, with little opportunity for training due to the unprecedented scenario.

Phishing attacks increased significantly since 2020, with 48% of cases of cyber attacks in 2021, an increase of 7% (HKCERTCC, 2021). For schools in Hong Kong, the adoption of e-learning was accelerated, and technological integration was not a seamless action, with phishing attempts hindering school planning. Reactionary planning strategies offered few opportunities for cybersecurity awareness training for school stakeholders. Inadequate preparation for students to manage their online behaviour made school stakeholders vulnerable to attacks. Phishing attacks on educational institutions have seen a significant rise (Gov.UK, 2023), and there are gaps in students' knowledge of how to protect themselves to minimise the impact of cyber attacks. Data was unavailable for Hong Kong; however, only 62% of secondary schools provided staff training and less for students regarding phishing (Gov.UK, 2023). There is also limited scope in how students can mitigate phishing attempts or be cyber-aware, whilst the threats can have physical, emotional, and social repercussions.

The project aims to understand the cyber awareness of Secondary school students in Hong Kong regarding phishing and evaluate the students' response capabilities. The objective is to

increase student efficacy in managing online behaviour, particularly in detecting potential phishing attempts and managing personal data effectively. The audience is aimed at secondary school students; however, this extends to parents, academic teaching staff and cyber security researchers as research considering the age range of students is limited and also students in Hong Kong particularly. The writer has a personal interest in Hong Kong education practices from a teaching position and has had the opportunity to witness the transformation of the education system with schools and students depending on e-learning platforms. With Hong Kong's unique landscape of blended Western and Eastern cultures and advanced technology infrastructure, students must be cyber-aware. This identification was noticed in the school environment in numerous schools. As an educator, it is necessary to provide students with skills, awareness and tools to empower them as digital citizens and contribute to a safer, secure society in the future.

The scope of the project aims to examine the challenges of integrating technology into school curriculums as the e-learning transition has not been cohesive. However, the flexibility and convenience of e-learning have resulted in increased school adoption. The scope extends to consider the state of cyber awareness of students and how they practice their online behaviour concerning phishing attempts. Data collection involves a developed web application, https://projectphishing.com, to assess participants' self-efficacy and cybersecurity awareness. Participants undertook a phishing simulation to guess which emails were genuine or phishing attempts correctly. The process concluded with another questionnaire to reflect on their cyber awareness behaviours and the simulation. Participants are given a performance score and recommendations to support positive digital citizenship.

This research project aligns with the area identified in the Cyber Security Body Knowledge (CyBOK) in Cybersecurity Human Factors Cybok 4.2, 4.4 and 14.6 (Martin et al., 2021).

2.0 Background (2818 words) - Critical Review of Literature

Due to the general advancement in technological contributions, the education sector has rapidly adopted new technologies to support teaching and learning. The adoption offers many opportunities for schools to transform teaching and learning; however, it also presents challenges to implement. Schools have long adopted e-learning as a supplementary tool to support traditional teaching methods; however, in recent years, it has become pivotal to secondary schools, particularly in Hong Kong.

Integrating e-learning into schools has transformed teaching practices; however, using digital platforms offers the risk of cyber threats. In this literature review, we aim to understand the issues of integrating e-learning in schools, the challenges for schools that adopt e-learning and the measures needed to protect students from cyber threats and become responsible digital citizens.

2.1 Defining e-learning for school integration

E-learning refers to the learning that takes the place of used resources, which goes beyond technology (Sangrà et al., 2012). Sangrà et al. (2012) suggest that e-learning enhances technology-driven education with a focus on learning resources. Garrison (2016) views e-learning as a disruptive technology (Garrison, 2016), transforming how learning is approached, contrasting with Rodrigues et al. (2019), who suggest it provides personalised, learner-centred, interactive learning experiences. The diversification of e-learning platforms can complicate matter that offers susceptibility for cyber threats like phishing (Rodrigues et al., 2019).

A consistent e-learning definition can ensure quality education as educators share a common understanding of implementation. Inconsistent consensus of definition causes conflict with teachers' ideas of implementing technology in school curriculums and can be challenging to assess the efficacy of e-learning programs. Inconsistencies from stakeholders can make schools susceptible to cyber attacks like social engineering attempts, whereby human psychology is targeted more than system vulnerabilities.

Definitions are significant for policy development and regulations by educational institutions to provide quality education and can provide the basis for security frameworks to be designed. Therefore, the evolving e-learning definition challenges educational institutions to address cybersecurity concerns, as integration becomes complex when aiming to safeguard stakeholders.

2.2 School institution's response to adopting e-learning

Hong Kong schools rapidly adopted e-learning into schools due to school pandemic suspensions. Teachers adopted e-learning autonomously, which led to inconsistent outcomes due to a lack of training for teachers not permitting effective teaching and learning. Online safety lessons have been left to teachers to decide how and if the content should be taught (Hartikainen et al., 2019). Hartikainen et al. (2019) found that teachers expressed the need for support, feeling unqualified to offer effective teaching. As much as 44.2% of students in Hong Kong felt e-learning was not as effective as face-to-face learning and slowed their academic progress. Harris (2016) emphasises the importance of allowing teachers to be part of the decision-making process in implementing e-learning to support policy, which could empower them to adapt their traditional teaching methodologies (Harris, 2016). The lack of preparation inadvertently meant that students and teachers became a target for cyber threats, including phishing attacks, with over 95% of IT infrastructures unable to protect their institutions or students (Shaikh et al., 2023).

The social need for learners was identified as a concern with a more significant digital divide between students and staff (Ng et al., 2020). Many students could adapt quicker to e-learning than teaching staff with data privacy concerns identified. The divide is a vulnerability, with 45% of technology students lacking the awareness to identify and counteract phishing attempts (Alhaddad et al., 2023). While most technology students could identify the threat, they did have technological awareness, while students in this study are far younger. The views of Harris (2016) and Ng et al. (2020) signify the issue of whether educators alone can bridge the digital divide.

Schools in Hong Kong have adopted e-learning support by the Education Bureau to offer students a blended learning approach (Ho et al., 2020) and support learning when extraordinary

situations arise, such as pandemics, high sickness rates or extreme weather. Ho et al. (2020) identified that the average frequency of using e-learning on a typical school day is 1.88 hours, which can rise to 4.72 hours during face-to-face school suspension times. Further research is required to understand the current e-learning hours for students now that the school suspensions are over; however, blended learning styles are now common and part of school practices. Ho et al. (2020) support this, suggesting that teachers should use e-learning tools to encourage personalised learning, reduce teacher-oriented approaches, relieve teacher pressure, and give them appropriate training and support.

2.3 Challenges posed by e-learning

Integrating technologies into school curricula is now familiar to students and staff (Turnbull et al., 2021) in various software applications and e-learning platforms. However, whilst software applications are familiar, online competence is an issue with inconsistency towards privacy, confidentiality and social engineering mitigation. Turnbull (2021) identifies a lack of digital literacy across subject departments that can leave students and staff vulnerable to malicious attacks, notably phishing.

Turnbull (2021) highlights the issues of digital illiteracy at higher educational levels, suggesting that digital literacy may be a concern from secondary schooling. With limited research on this area in Hong Kong secondary schools, a pronounced risk is identified due to the under-researched secondary school level focus area. From understanding the challenges of integrating technology into school curriculums and the increased adoption of e-learning by schools, we can comprehend the landscape to see how crucial these challenges are for students to be better digital citizens, manage themselves online and mitigate potential phishing attacks.

2.4 Cyber Awareness of Students

In the research context, the focus population is secondary school students aged 11-18. Students may regularly use digital platforms, but their ability to recognise and mitigate cyber threats such as phishing can be a concern. Therefore, it is essential to explore students' knowledge of online protection to assess their cyber awareness and practices. Cyber awareness transcends knowledge as it aims to equip learners with skills and techniques to manage online behaviour.

The concept relies on human factors and influences on students to reinforce awareness of cyber attacks and promote digital citizenship (Antunes et al., 2021).

Zorlu (2022) suggests that internet users are more likely to be cyber-aware and that students often possess the necessary skills and knowledge to protect themselves online. The study utilises the research conducted on developing the Personal Cyber Security Provision Scale (PCSPS) (Erol et al., 2015). The Erol et al. (2015) scale supports effective measurement to analyse cyber awareness, identify trends in awareness, and determine whether precautionary measures are taken to protect personal privacy. The scale adequately supported Zorlu's (2022) findings that females possess higher cyber awareness, although 75.1% of participants were female. This does raise a limitation in the comprehensiveness of the findings. Further studies indicate that students have a good knowledge of cybersecurity risks, practices and tools (Nicholson et al., 2021).

Nicholson et al. (2021) challenge the point that good knowledge can be implemented initially; however, students seem to disregard the protective measures over time due to the usability of security. The emphasis is placed on practical application by Nicholson et al. (2021), which contrasts with Zorlu (2022), who suggests that awareness is enough to manage digital citizenship. Transforming students' good knowledge into practical application to demonstrate actual positive online behaviours is crucial. The Nicholson et al. (2021) study identified that teaching methods and school curriculums lack opportunities for students to apply the knowledge they can gain. In the study, students experienced live demonstration workshops for data collection, which was beneficial in identifying the knowledge. However, the limitation of students independently testing their knowledge in a practical setting meant they failed to understand the full implications of not consistently showing cyberawareness behaviour independently. The limitation of testing in the study may skew findings, and students may have behaved differently in participation compared to a real-life setting or a controlled workshop environment.

Zorlu (2022) and Nicholson et al. (2021) explore cyber awareness as a concept, yet there is a distinct research gap on the psychological effects of cyber threats on students. The opportunity to practice methods in a safe environment could have explored this area more thoroughly. The delivery of content from teaching staff was identified as an issue, with staff suggesting they lacked expertise and efficacy. Inexperience and lack of training would cause students to feel

overconfident if they were praised for increased knowledge. Knowledge gaps will be evident as technology evolves more rapidly than schools can offer training to teachers through limited resources and funds. Students are thrust into a technological lifestyle, and without trained teachers, students may unwittingly be inadvertently led to riskier online behaviours.

2.5 Cyber attacks on schools

Globally, the rising trend of cyber attacks on schools has continued, with ransomware attacks up 56% in 2023 from the previous year (Sophos, 2023). The motivation is to monetise the attacks; using stolen data through ransomware, phishing, and malicious emails can account for 30% of the root causes of attacks in secondary schools globally. This may not be the most common attack; compromised credentials, malicious downloads, and exploited vulnerabilities can stem from phishing. Sophos (2023) identified that the education sector is particularly exposed to attacks with reduced cyber readiness and defences compared to the technology and telecom sectors. In Hong Kong, reported cases of email phishing have reduced since 2022. However, phishing tests on adult employees indicated that cyber awareness is low and has room for improvement (SCMP, 2023a). Hong Kong students were reportedly involved in risky online behaviour, whereby 20% fell victim to online abuse and blackmail cases (SCMP, 2023b).

Due to the increased adoption of e-learning, vulnerabilities have emerged in e-learning platforms. Common vulnerabilities, such as weak password policies and a lack of multifactor authentication, can cause compromised credentials. Platforms running outdated software without the latest security patches leave opportunities for exploitation, and a lack of data encryption in storage and transmission has the potential to be misused or targeted for ransom demands. Stakeholders play a crucial role in minimising human error by identifying phishing emails and inadvertently compromising security policies. A stronger emphasis is on training stakeholders to have good knowledge of operating platforms to identify areas of concern, prevent potential breaches, and offer parameters to reduce human error, such as sharing passwords, clicking links in phishing emails and monitoring control access (Akacha & Awad, 2023).

2.6 Phishing attempts on schools

Phishing is a prevalent form of social engineering (Broberg & Sinnott, 2023) that disrupts e-learning. To place phishing in context and understand the severity, Hong Kong schools have fallen victim to cyber-attacks with reports of data leaks (Mok, 2019) and ransomware demands (Steed, 2023) following targeted phishing emails. The lack of security infrastructure in the education sector has increasingly been targeted through phishing attacks such as spear, whaling and deceptive phishing (Birlea, 2020) and suggests that deceptive phishing is often used to spoof or impersonate to steal credentials. Spear phishing is the most common target method for schools, with the aim being an individual or group of stakeholders, particularly students and teachers. (Richardson et al., 2020).

Higher education institutions are also targeted through similar phishing attacks, with concerns raised over a lack of cyber awareness (Liu, 2022) that prompted the Hong Kong Education Bureau to deliver workshops for schools as guidance to be vigilant on cybersecurity matters and strategies (Hong Kong Education Bureau, 2020). In conjunction with the United Kingdom (U.K.) National Cyber Security Centre audit findings revealed that over 83% of schools had experienced a cyber-incident, with phishing emails 69% the most prevalent attack, with only 35% of schools performing any training on non-IT staff sighting resources and cost as the reasoning for this (Irwin, 2023).

Hong Kong schools continue to be targeted by malicious users, such as more recent breaches involving data loss (Mycroft, 2023); the attacks are prevalent globally, with 91% of all cyber attacks initially starting with a phishing email to an unsuspecting targeted victim (Ho, 2020). The findings raise issues such as financial costs, privacy exposure and vulnerabilities from systems or humans. The reports fail to identify the psychological effect on stakeholders involved, loss of learning time to students and reputational damage to schools.

Disruption to e-learning through phishing can often be investigated by identifying students' self-assessments. Students who define the term phishing and understand phishing attacks are often more susceptible to falling for phishing emails (Diaz et al., 2020). The research from Diaz et al. (2020) implies that students with higher self-efficacy in phishing can overestimate their knowledge, contrary to original expectations. Whilst the participants were unaware that this was an experiment, 70% of the subjects had clicked on malicious links. This identifies that

phishing awareness is an underdeveloped area of research. In a more controlled environment, where students could have trained over numerous weeks, cyber awareness improved in the short term by 14% (Lastdrager et al., 2017).

Secondary school students could take great value in participation in simulations rather than live targeted phishing campaigns or workshops (Sağlam et al., 2023) to learn and progress in a safe and controlled risk environment. Simulations can replicate real-world situations safely (Zhang-Kennedy & Chiasson, 2021), emphasising educators' need to support curriculum changes with simulation strategies. However, simulations do not offer the unexpected challenges of real life.

Human error can allow cybercriminals to exploit system vulnerabilities, so strategic and operation planning and management are needed for a safe learning management system. Malicious criminals can passively and actively collect information from targets (Ruiz et al., 2023) and identify that training is necessary for staff using these platforms. School decision-makers need to pay attention to and not over-trust platforms.

Technological tools and applications will evolve; however, human interaction will remain a constant variable. School leaders applying technology or application platforms alone is insufficient to build a cybersecurity culture. There should be a collective responsibility across the school's stakeholders, from the student to the board.

2.7 Protection against phishing

Innovative measures such as the successful Wise-It-Use (WIT) program emerged in Hong Kong (Chau et al., 2019), implying that gamification could increase students' cybersecurity knowledge and foster positive online behaviour through gameplay activities. The debate continues on whether gamification in cybersecurity would be as effective for diverse populations of students globally. Gamification can improve engagement levels; however, the concern is how far they prepare students with a deeper understanding to mitigate a real-life cyber threat, which entails actual consequences which a game cannot offer.

Self-efficacy can support a protective online lifestyle to mitigate phishing attempts (Lee et al., 2023). A dual perspective suggests that users can gain knowledge to have self-efficacy and

empowerment, yet knowledge can breed overconfidence and risky online behaviour. Lee et al. (2023) continue that those with higher self-efficacy will be more likely to protect their personal information online and show a good attitude towards online behaviour, meaning they are less likely for victimisation. The study by Lee et al. (2023) was not confined to Hong Kong, and participants had a greater age range with an unaligned comparative demographic. Therefore, identifying trend patterns with gender and focused age range could be valuable.

Globally, school curriculums inadequately educate students on phishing (Henshaw, 2023), leaving them vulnerable in real-life situations. Students could aim for higher self-efficacy in cyberawareness, which may support other societal sectors, such as financial services or business.

Technical security measures offering a multi-layered approach to school protection, such as email filtering, would support; however, using machine and deep learning technologies could offer a comprehensive strategy to identify potentially malicious emails (Bagui et al., 2019). Machine learning and artificial intelligence can be used to classify phishing attacks and understand the provisions needed for schools (Seth & Damle, 2022); however, humans would need to manage these technologies, and currently, there seems to be a lack of provision for this in the education sector. Providing students and teachers with regular training sessions and simulated phishing tests will provide effective responses in readiness to respond well to phishing and have an elevated cyber awareness (Chowdhury & Gkioulos, 2021). Chowdhury and Gkioulos (2021) found that research and development simulation training would increase awareness, but real-life testing is preferred. Debate exists on the consensus for the most effective method to offer protection as software applications accumulate high costs, gamification is engaging but time-consuming, and simulations can replicate real life but require existing knowledge (Chowdhury & Gkioulos, 2021).

2.8 Conclusion

A deeper understanding is necessary to understand how students can translate theoretical knowledge into practical security-based behaviours. As the digital technology landscape increases for schools, more opportunities and vulnerabilities may be presented for malicious users. A holistic approach is needed to provide cyber awareness policies and curriculums to engage students and provide them with online tool protection. Technological interventions such as spam filtering, artificial intelligence detection, and security audits may not be enough to mitigate phishing attempts and avoid facing the consequences of a cyber incident. Therefore, equipping students with understanding so they can practically manage themselves through fostering a culture of cyber awareness.

3.0 Ethical and Professional Considerations (884 words)

Ethical and professional considerations are crucial to ensure the integrity of the research project, mainly due to the under-18 age targeted sample group of secondary school students with limited research carried out in this area (Unchit et al., 2020). The geographical location of Hong Kong is distinctive from other studies as no other research was found from this location.

Engaging with a younger population offers a privileged insight into understanding the nature of phishing awareness, as age has been considered a determining factor in predicting susceptibility to phishing attacks (Nicholson et al., 2020) and potential harm and influence. The opportunity for participants to opt-in to the research was provided to 897 students, hoping to gain perspectives on human behaviour contrasting from adult populations. The research adopts a cautious approach to protect participants' wellbeing at the core focus with informed consent and protected data collection. As a registered, experienced teacher, safeguarding students is paramount and every effort was taken to minimise potential risk and protect student wellbeing.

The Hong Kong Secondary School authorised a signed document (Appendix 1) to allow the data collection to proceed with participants. The involvement of all stakeholders (students, teachers, student wellbeing team, leadership team, parent/guardians, school board) within the school community recognises the ethical implications reach far beyond the participants even though they are focal points. The collaborative approach reflects compliance with procedures and a commitment from all stakeholders who see the benefits of the research project.

Participants were first asked to participate through a prepared video (Appendix 8) in their respective year assemblies so all students could be messaged simultaneously at different venues, and all had access to the advertisement. The student population were offered a letter of consent (Appendix 2), a detailed participant information sheet, a parent/guardian information sheet (Appendix 3) and a snapshot information sheet (Appendix 7). The consent letter emphasises the rights and processes to confirm the transparency of the research and the data to be collected. The snapshot information sheet was a differentiated resource that provided essential information more understandably to cater to students' learning abilities and needs (Figure 1). The resources were a supplementary addition for the participants rather than a substitute. The comprehensive approach aimed to demonstrate dedication to inclusion,

accounting for a broad ethical vision, and cater to all participants engagingly regardless of age and literacy level.

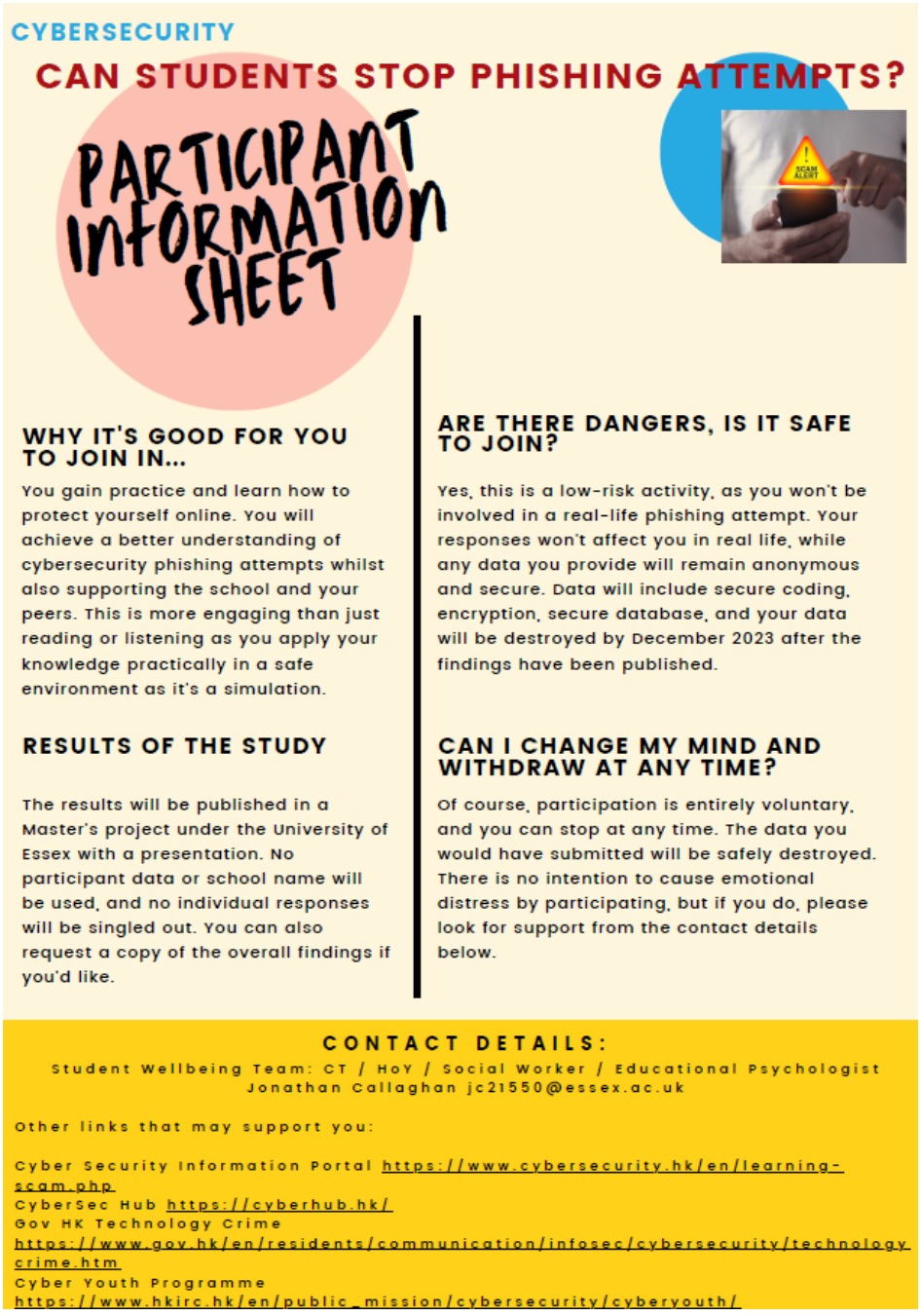


Figure 1: Extract of snapshot sheet

Phishing involves deception, which raises a significant concern with younger participants that can trigger negative psychological responses (Goel et al., 2017). All participants were instructed on the deception concerns and potential impacts that could arise from conducting

the research in acceptable conditions. Ssimulation deception is explained to participants and is not expected to cause harm or emotional distress (Boynton et al., 2013) with further support websites, email and phone contacts provided should participants require intervention, and the school wellbeing team with social workers and psychologists are available on request.

The debriefing following the simulation offered participants a platform for support to communicate concerns, gain reassurance, and ensure that any deceptive elements of the research did not leave any negative and lasting impressions. The collaboration with the School further offered support from the Student Wellbeing Team staff (Heads of Year, educational psychologists, and social workers), who were available to support specific concerns or emotional distress depending on the level of intervention needed.

Participants will be briefed regarding the consequences of misusing information presented in the simulation to mitigate inadvertent negative learning. Instruction explicitly highlights the unethical and potentially criminal damages of using phishing knowledge, negatively reinforcing the research objectives and eliminating misconceptions.

The information sheets clarify the nature, how the data will be collected, and potential risks identified. Data will be stored in a cloud database (Appendix 13) that identifies six data tables that will be collected and used. Unique identification numbers are used to protect personal data, and data is anonymised with password hash encryption. All data will not be kept longer than deemed necessary and destroyed after the project has been submitted and published.

The research follows best practices concerning professional practices with efforts to reduce the likelihood of data breaches through adequate security and privacy control implementation. Data breaches in Hong Kong are not statutory defined under the Hong Kong ordinance, and there is no mandatory requirement for data users to notify subjects or authorities (PCPD, 2023); however, there is non-binding guidance issued encouraging notification to authorities and data subjects could be harmed if they were not informed. The project followed this guidance for best practices and would inform participants and authorities.

Adhering to ethical concerns, professional practices were considered following the BCS Codes of Conduct (British Computing Society, 2022) and ACM Code of Ethics ((Association for Computing Machinery, 2023)). Data will be stored in a secure third-party cloud database that

has been vetted, secure, and reliable. The provider has built-in mechanisms for up-to-date patches and recovery. The artefact web application was designed using the Python Flask framework's security libraries. Adhering to these standards amplifies the credibility and ethical standing to align the research to demonstrate integrity and responsibility. The research project is invested in upholding ethical and professional practices to balance the research objectives with participants' vulnerability to produce fair, reliable, valid findings with consideration of the subjects involved.

4.0 Main Body (3730 words)

4.1 Introduction

The integration of e-learning in secondary schools has presented new challenges in cybersecurity. The research addresses how cybersecurity awareness can empower secondary school students to mitigate phishing attempts during e-learning. The methodology details the research design to justify using a simulation as a cybersecurity tool and providing a profile of the participants involved. A phishing simulation artefact details the process undertaken to design and execute the simulation whilst identifying the method for collecting data. Discussion will take place on the techniques used for data analysis to show findings to identify quantitative and qualitative information on students' responses to phishing attempts, showing descriptive statistics to support in-depth analysis of patterns, trends and group comparisons. Interpreting the findings relates to the literature review, understanding significant implications for e-learning and Hong Kong schools and limitations that have affected the research. In concluding remarks, recommendations will be offered for schools with suggestions of areas to continue future research in this area.

4.2 Methodology

4.2.1 Research design

The phishing simulation is designed to act as a training tool for students in preparation for or undertaking e-learning. The choice allows students to participate in a controlled environment representing real-life cyber situations, not incur genuine risks and lasting consequences. Students are exposed to the deception of phishing without falling victim to potential data theft, financial loss or harm. Simulations offer adaptability that can be tailored to meet the needs of the demographic, education levels, and the school environment in Hong Kong. Quantitative data collection, such as identifying if the email was phishing or not and clicking phishing URL links (Figure 2) and qualitative data can also be collected, providing reasons for justification of email decisions.

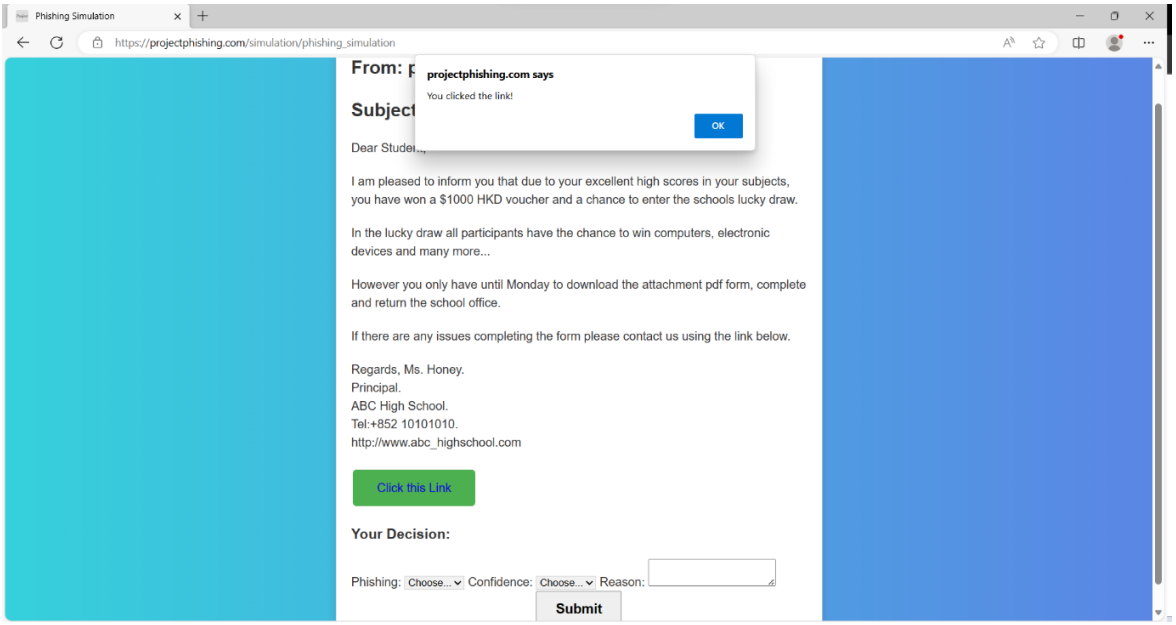


Figure 2: Email challenge with a URL link

The design of the simulation stemmed from crafting emails similar to emails that students would regularly receive through their e-learning platforms. The research identified commonly used spear phishing strategies to target emails towards students (Stanford University IT, 2023). Designing relevant and related emails was significant so students could relate the simulation to real-world scenarios in a controlled environment. Figure 3 shows a phishing email designed to deceive the student into clicking a link that could potentially have negative consequences. Similarly, design concepts can be evident in research (Maharishi School, 2018) with characteristics that deem the email a phishing attack. Techniques such as 'no reply' in the address link suggest the intended recipient cannot query the overdue book.

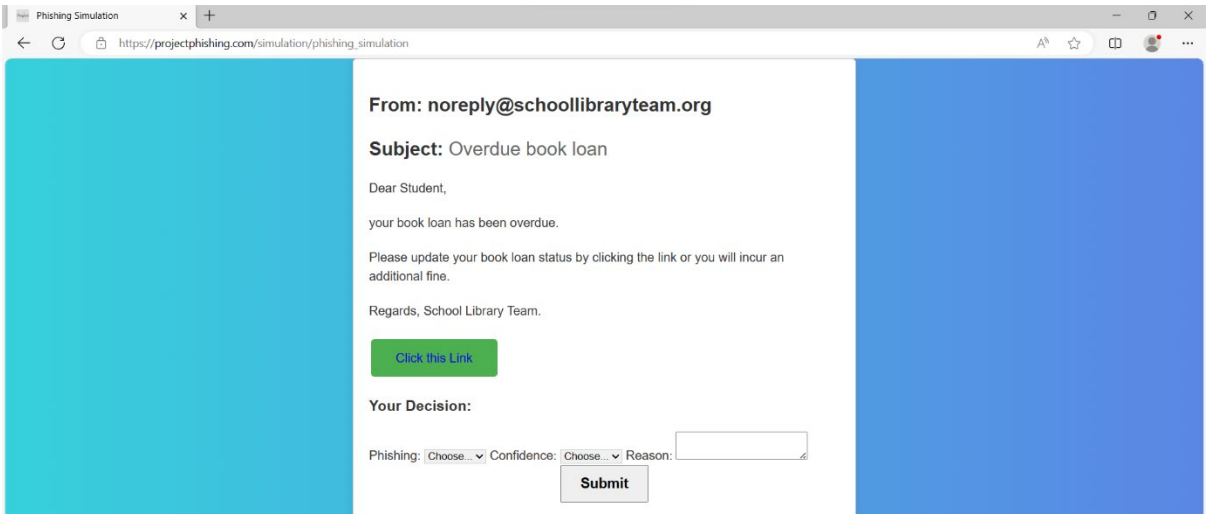


Figure 3: Example of phishing email allegedly from the School Library team

School emails can be automated, and suspicion is raised over the lack of personalisation to the student, notably 'Dear Student', with no details of the book title in question nor the duration of the loan. The lack of capitalisation of 'your' with a threatening message of the risk of an additional fine suggests a psychological element that the student has already incurred a fine. This may place more significant anxiety and urgency on the student and cause an irrational decision. The example identifies traits similar to TA407/Silent Librarian (O'Donnell, 2019), asking students to click an urgent link to take action. O'Donnell (2019) suggests that the typical social engineering technique usually redirects users to a fraudulent website that looks legitimate, and victims' credentials are often stolen. The approach known as sending a 'knock door' email (GreatHorn, 2020) to establish a connection with the target can be as simple as a brief introduction or more sophisticated (Figure 3).

Six simulation emails were designed with two genuine and four phishing. The email challenges were given a tracking identification number to analyse the most effective emails on deception. The content of the emails was placed in the cloud database for seeding (Figure 5).

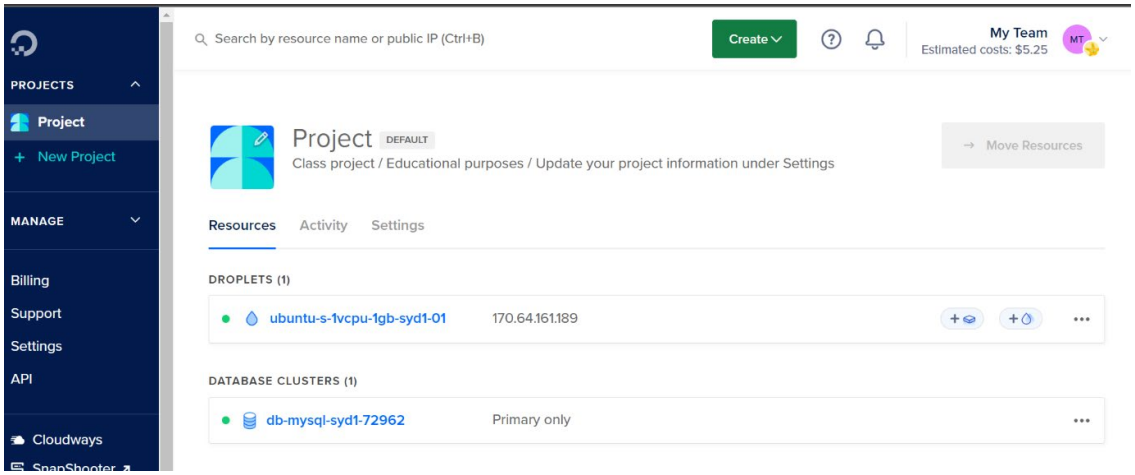


Figure 4: Server and cloud database

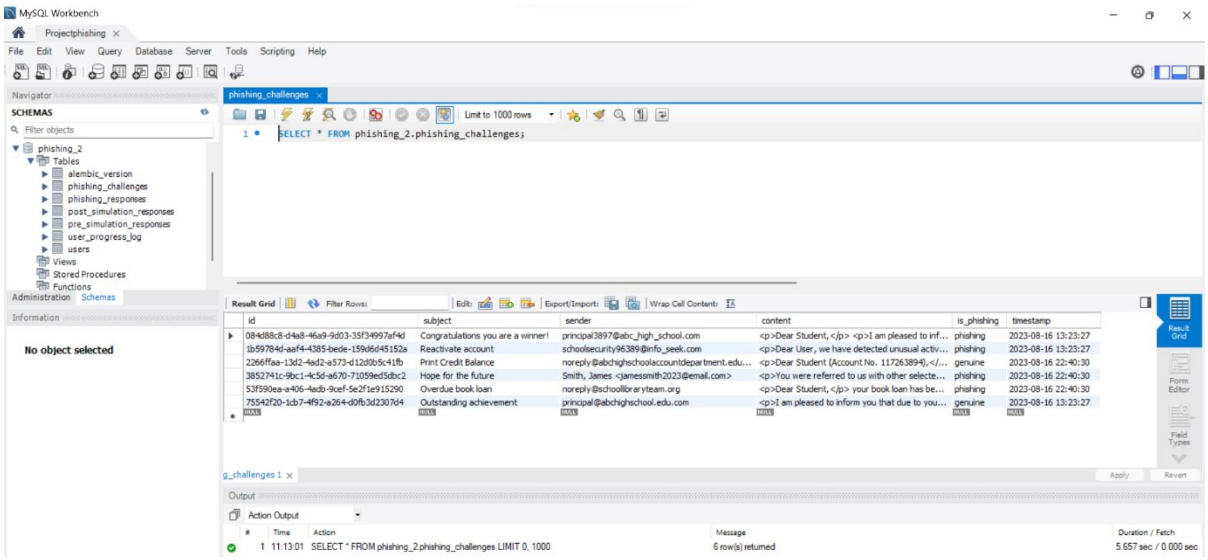


Figure 5: Phishing email challenges for the simulation seeded in the database

The number of emails was limited to six as the 11-18 years age range was broad for high school students with mixed education abilities. The aim was not to overload or cognitively stress the students with too many challenges. The ratio of genuine to phishing emails is 2:4, with various phishing techniques in differing contexts that could be explored to support cyber awareness training. As this was not a live environment and students were aware this was a simulation exercise, students tended to scrutinise the emails for social engineering techniques; therefore, the greater scope of techniques allowed more exposure for them.

Two questionnaires were designed to be completed before and after the phishing simulation. The Pre-Simulation Questionnaire (Appendix 4) collected the age and gender of the students, asking them about their experience, knowledge, and confidence in managing phishing. The Post-Simulation Questionnaire (Appendix 5) was required immediately after the simulation, and data was collected on the students' perceived performance in mitigating phishing emails and reflecting on the simulation process. All data was collected in a cloud database that tracked if links were clicked on and students' decisions on the email challenges.

From an ethical stance, a crucial activity was the debriefing that followed the Post-Simulation Questionnaire. The debrief was conducted in two parts; the first part identified participant performance scores. The grade level boundaries were designed based on the NIST Phish Scale to provide context to phishing data and support a better understanding of why people fall victim to such attacks (Barrientos et al., 2021). The NIST Phish Scale uses a five-point scale to identify

cues to suggest if the email is an attack and to distinguish how difficult it is to detect given its context. The output score would suggest the detention difficulty of the email (Dawkins & Jacobs, 2023). Considering the students' educational level, the concept of the NIST Phish Scale was considered in design; however, it was not directly used as it was deemed that analysis in the Post-Simulation review might be too challenging for younger or lower-ability students. The grade level boundary scoring was linked to the school attainment grade boundaries as this seems to be a fair reflective model to which the students were accustomed. In addition to the score and grade level, cues were highlighted in different colours to categorise the phishing tactics with short explanations for justification for each email.

The second part of the debrief (Appendix 6) provided feedback regarding the simulation's ethical and cybersecurity concerns to confirm that all participants knew the nature of the deception activity. Participants could ask questions and provide insights on identifying cues in potential phishing emails in real life. As seen in the information sheet, participants were provided with further information and more resources to support their cybersecurity awareness and education in Hong Kong.

Independent variable: Phishing attempt on the Secondary students.

Dependent variable: Decision made through the level of cyber awareness to mitigate phishing attempts.

Hypothesis – Secondary school students in Hong Kong have cyber awareness to mitigate phishing attempts.

4.2.2 Participants

The research participants comprised secondary school students in Hong Kong between 11 and 18 years of age. Recent studies suggest that younger people are likelier to be victims as they trust online communication more (Alkhalil et al., 2021); the sample is a relevant group to consider for phishing susceptibility.

The selection criteria for participants were open to all 897 students at the Hong Kong Secondary School between the ages of 11 and 18. All participation was voluntary, informed

consent was obtained from all participants, and all students provided consent from a parent/guardian. Whilst the age range may cover a range of learners, the prior knowledge of cybersecurity and information technology was mixed and assumed a low level. As the school offers technology integration in the curriculum, there are limited specialised Information Communication and Technology (ICT) lessons in the 11-14-year-old age group. Directed ICT teaching contact hours are lower than in other schools; however, students take the subject at the public examination level from ages 14-18. Generally, students have limited cybersecurity learning opportunities, with some lessons covered in Personal Health and Social Education (PSHE). This will support findings as students will demonstrate signs of self-learning or innate detection abilities when faced with phishing attempts rather than learning previous phishing cues.

Only 47 opted to participate, and one student did not fully complete the simulation on the day, so the results were omitted. A total of 46 participants (Figure 6), of which 27 were male (59%) and 19 were female (41%).

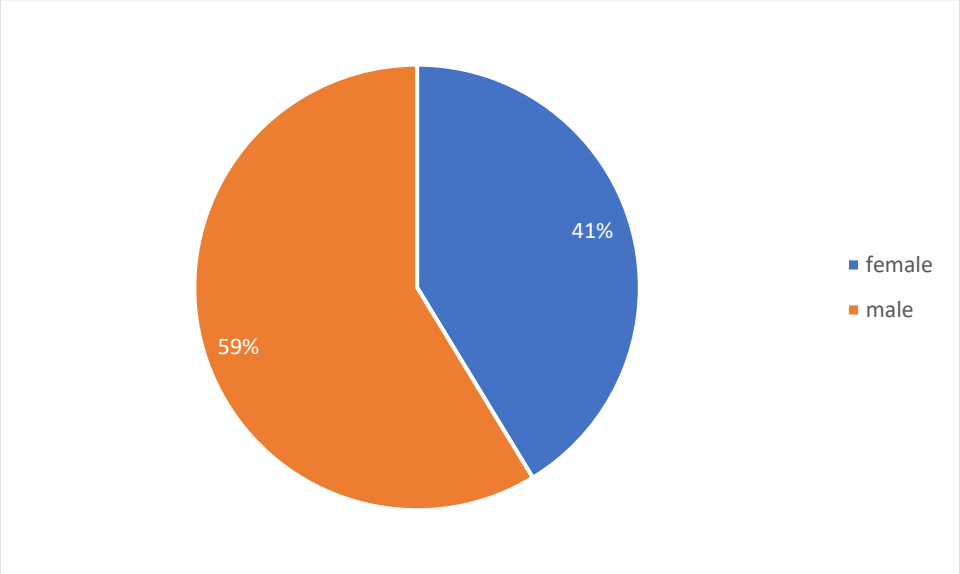


Figure 6: Chart showing the gender distribution of participants.

To compare the gender ratio for Hong Kong students who studied ICT at the public examination level HKDSE in 2022, males accounted for 76.2%, and 23.8% were female. The sample population has aimed for a balanced gender representation; however, it would be helpful to understand the context of gender representation of students who continue with ICT further studies. Whilst there was not balanced gender representation, the ratio was better than the gender ratio for ICT public examination candidates. The limitation of the study is that only 5%

of the School opted to participate. This presents challenges to gauge representative findings on students in Hong Kong. The youngest year groups, 11-12-year-olds, did not participate; many were new to the school, and as this was advertising during the first week of the academic year, the volume of advertised activities and consent letters sent to them may have been overwhelming. All participants who did opt in were 13 years old and over. The sickness rate was high for three weeks, with approximately one hundred students and staff absent daily. Numerous students forgot to return consent forms or did not participate well enough. The mean age of participants was 16 years, with a standard deviation of 1.2 years. The sample does not have a vast range, which affects the findings; however, we can understand findings of student cyber awareness, gender and age comparisons despite the limitations.

4.2.3 Artefact: Phishing simulation

The repository for the phishing simulation can be found in Appendix 14, and Table 1 shows tests for data analysis.

Table 1: Compilation of differing tests and the conditions of each test for comparison of the studies to be carried out.

Test / Analysis	**Comparison of conditions of each test/variable**	**Objective of the test**
Descriptive analysis	Age and Overall score	To find the demographic details such as average age and range.
Gender distribution	Males and Females	To show the gender representation
Cyber awareness training	Yes and No	To find the number of participants with cyber awareness training
Knowledge of phishing	Yes and No	To identify the amount of participants who were aware of the nature of phishing.
Confidence	Overall, Male and Female	To identify if gender has significance to confidence levels.
t-Test Phishing knowledge	Yes and No	To understand if prior knowledge of phishing impacts performance.
t-Test Gender	Overall Score, Male and Female	To find the relationship if gender impacted overall scores.
Correlation between age and overall score	Age and Overall Score	To find if age correlates to the overall scores achieved.
Regression for age and cyber awareness	Age and Phishing	To find if age can be a predictor of awareness
Email challenge accuracy	Count and accuracy	Identify the varied challenges
NIST Phish Scale	NIST email rating and data collection results	Aim to benchmark the email challenges against levels of difficulty

The participants were offered three time slots to visit the venue for the simulation, which was well-lit, with glass windows as walls and plenty of space. Teaching supervisors and myself were available to support participants. The timing was on a special shortened timetable day in the early afternoon after lunch, which was significant as participants were hydrated and fed and not exposed to an extended school day to ensure they were both physically and mentally prepared to undertake the task. All participants entered in good spirits and were eager to participate. The school has a bring-your-own-device policy (BYOD), and students could access the website for the research project (Figure 7) as they were connected to the school's Wi-Fi network.

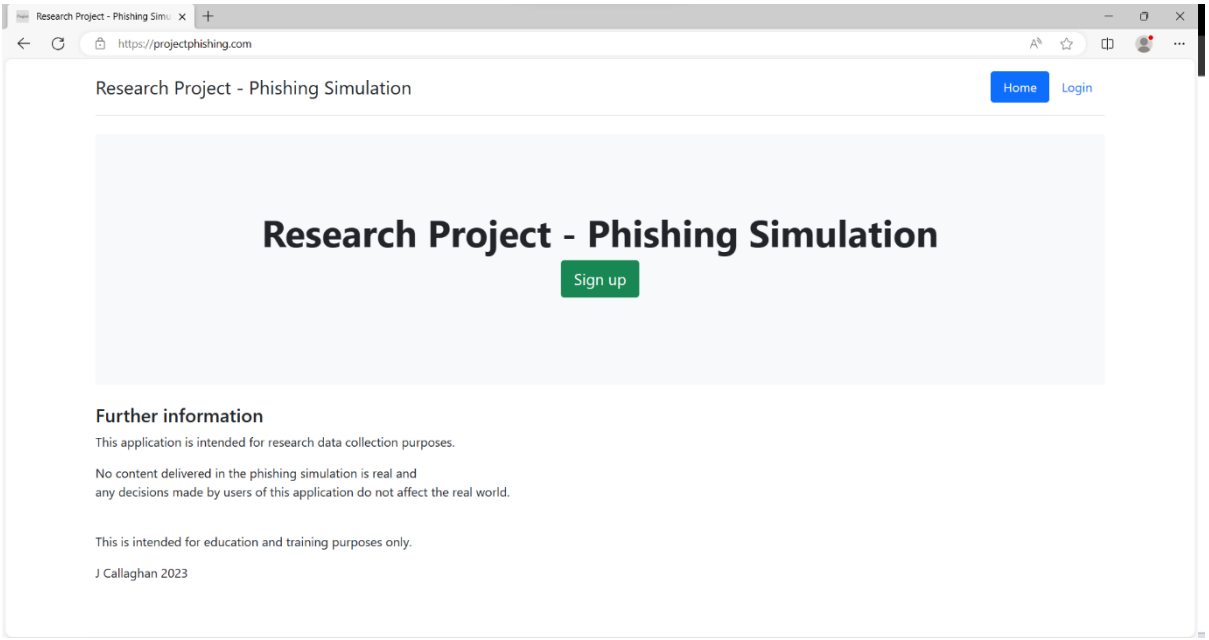


Figure 7: Home page of the phishing simulation web application

School-owned electronic devices were available if any students had device or connection difficulties; however, none were needed. Participants completed the simulation in silence, and once completed, they waited for the debriefing session.

Upon navigating to the home page, participants were required to register a username and password (Figure 9) that demonstrated good security practices for passwords and was memorable for them as the concept was that they could return to complete the simulation as training in the future to show progress (Figure 8).

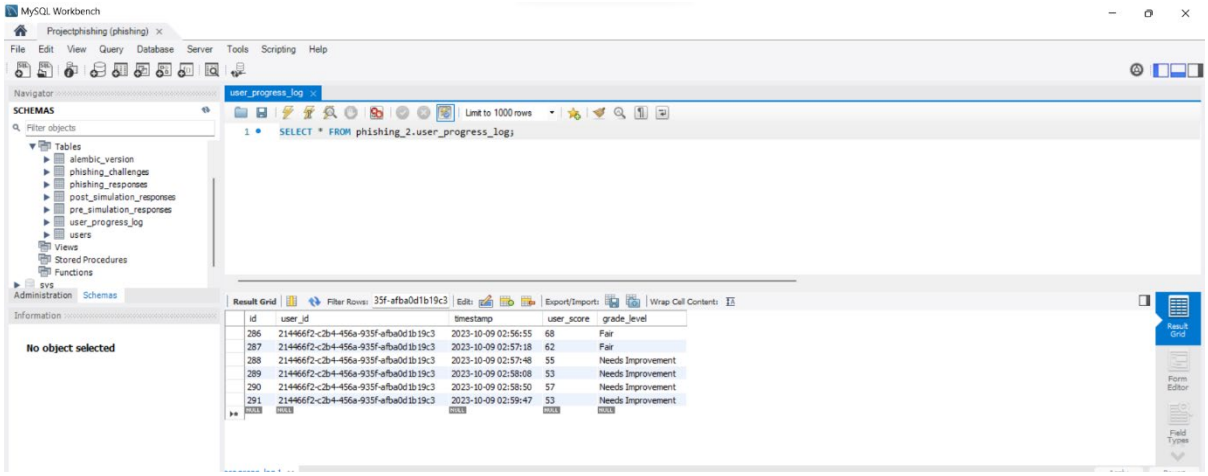


Figure 8: Progress log - User scores from each simulation challenge

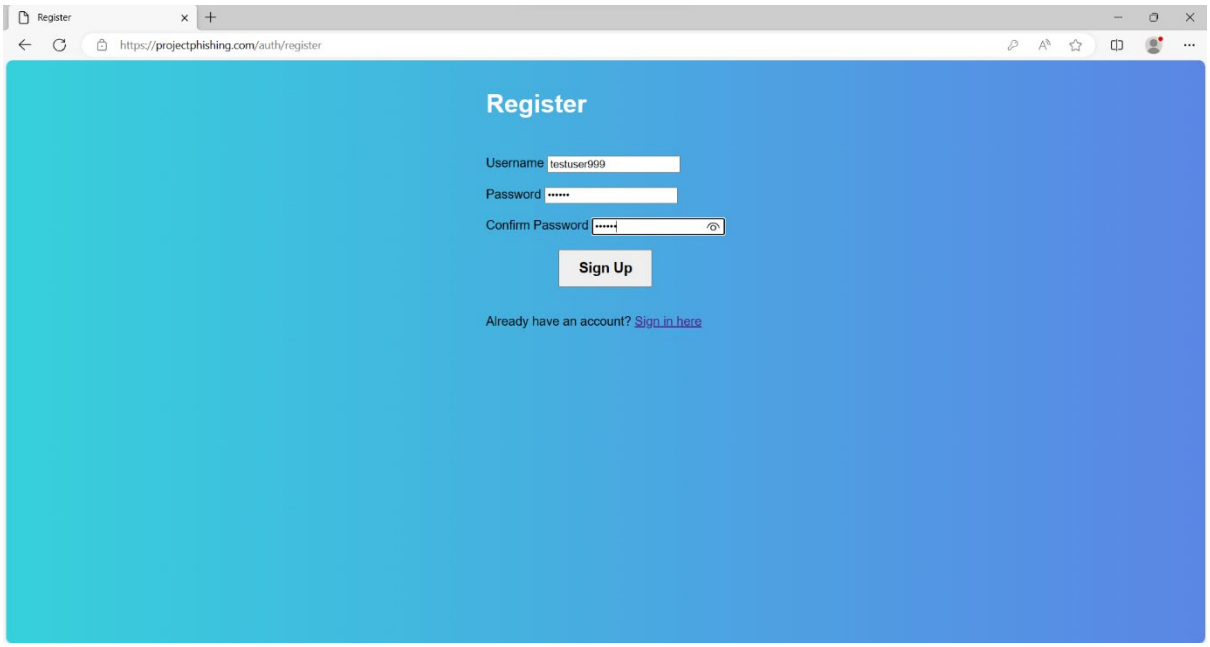


Figure 9: Participant registration

After successful registration, the user was redirected to a login page (Figure 10) to confirm that the credentials had already been created.

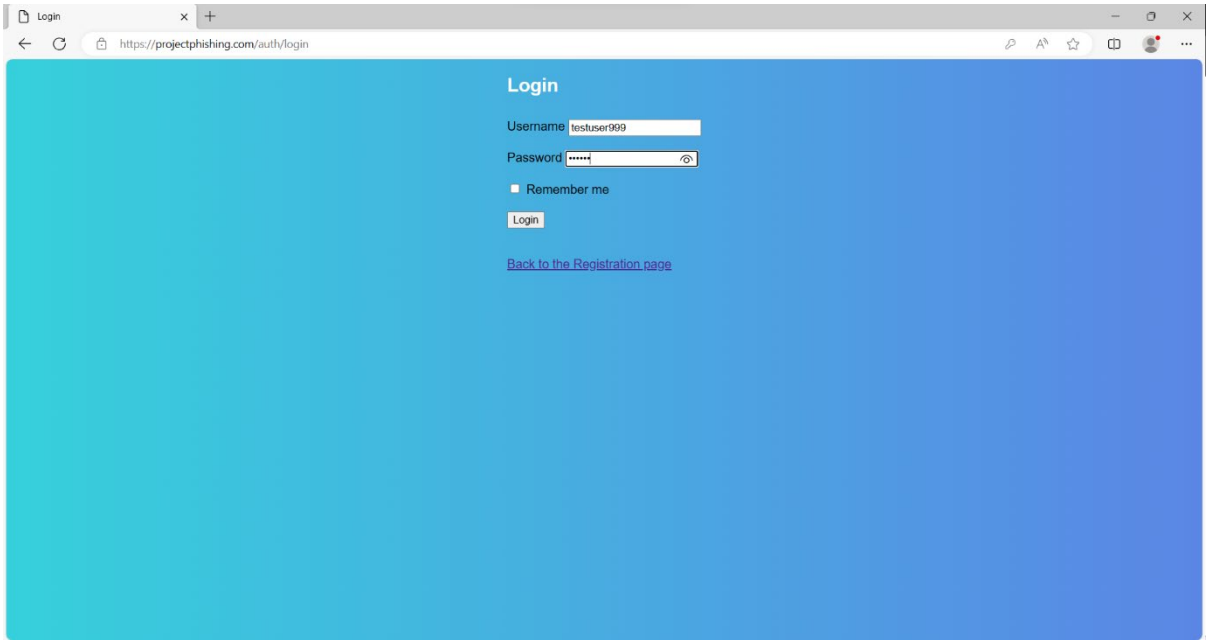


Figure 10: Login page

Unsuccessful logins would provide an error message to the user. Successful logins would redirect to the base page of the application (Figure 11).

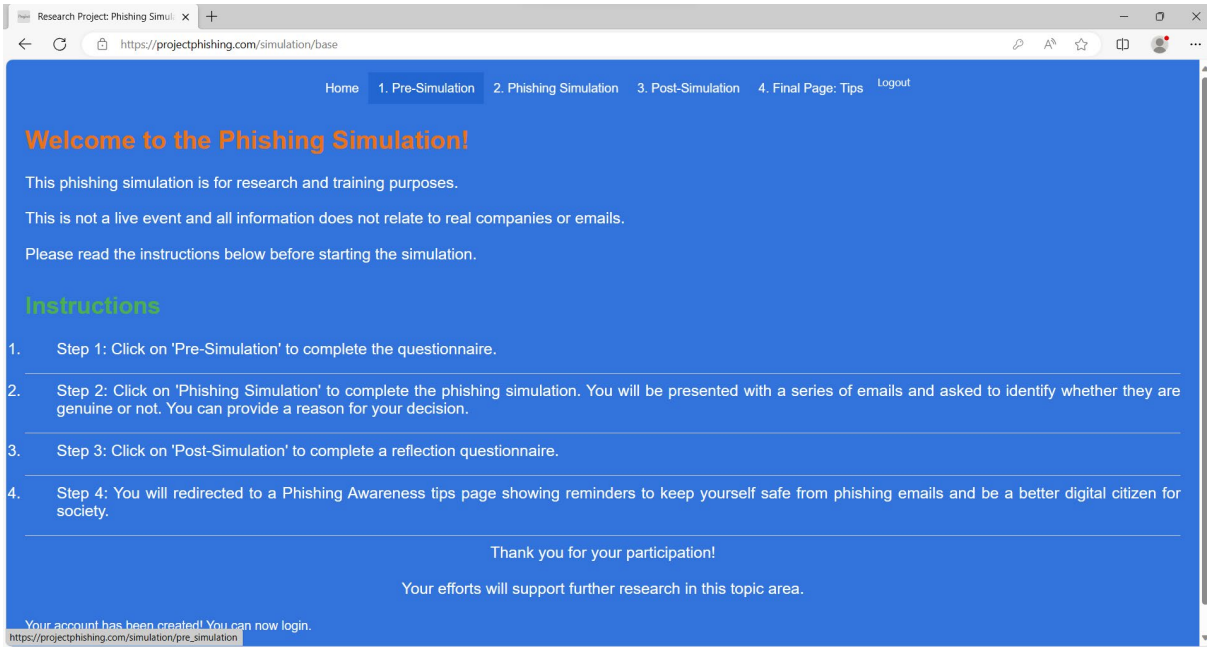


Figure 11: Successful login and base page

The participants were encouraged to read all information on the base page before proceeding to Step 1. Pre-simulation (Figure 12) was a questionnaire form to collect prior knowledge and the user expectations of the study.

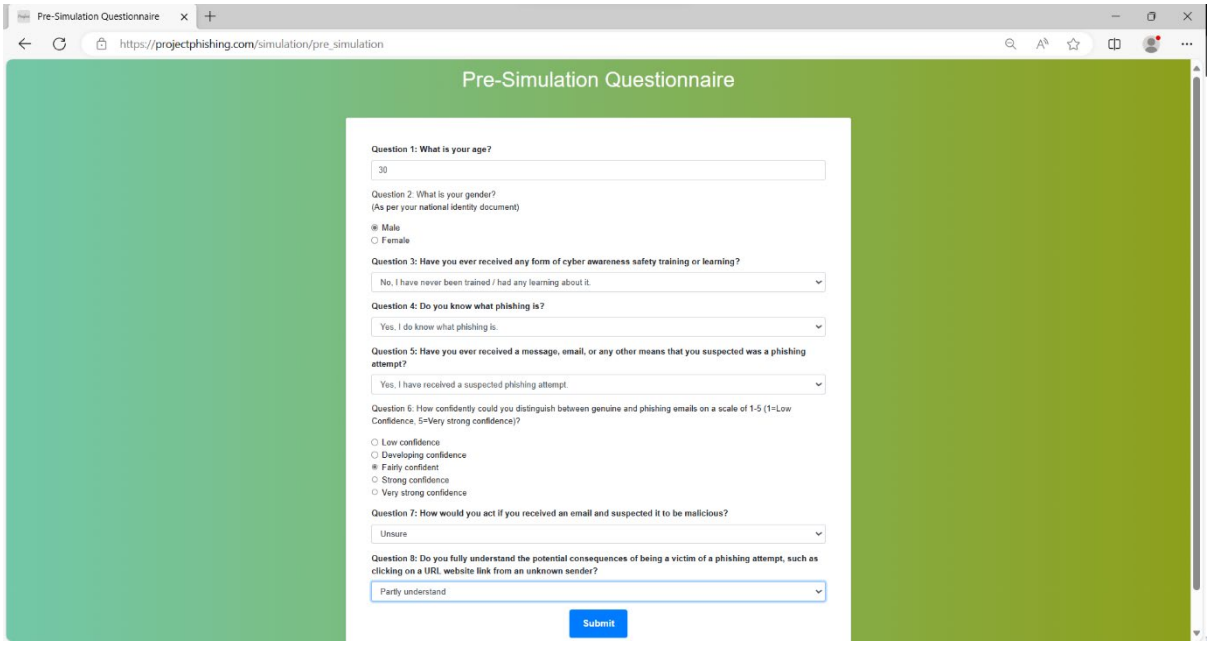


Figure 12: Pre-Simulation Questionnaire

Validation error prompts would message the participant for incorrect entries, and all entries allow form submission. Once completed, the participant was redirected to the base page again (Figure 13). The participant could check the instructions once more and have the opportunity to ask any questions before completing the simulation. Participants were informed that the phishing simulation would be timed in seconds per phishing email challenge and that a score would be provided at the end of the process, incorporating the decision-making duration. The time score attributed to 20% of the score for the challenge (Figure 14).

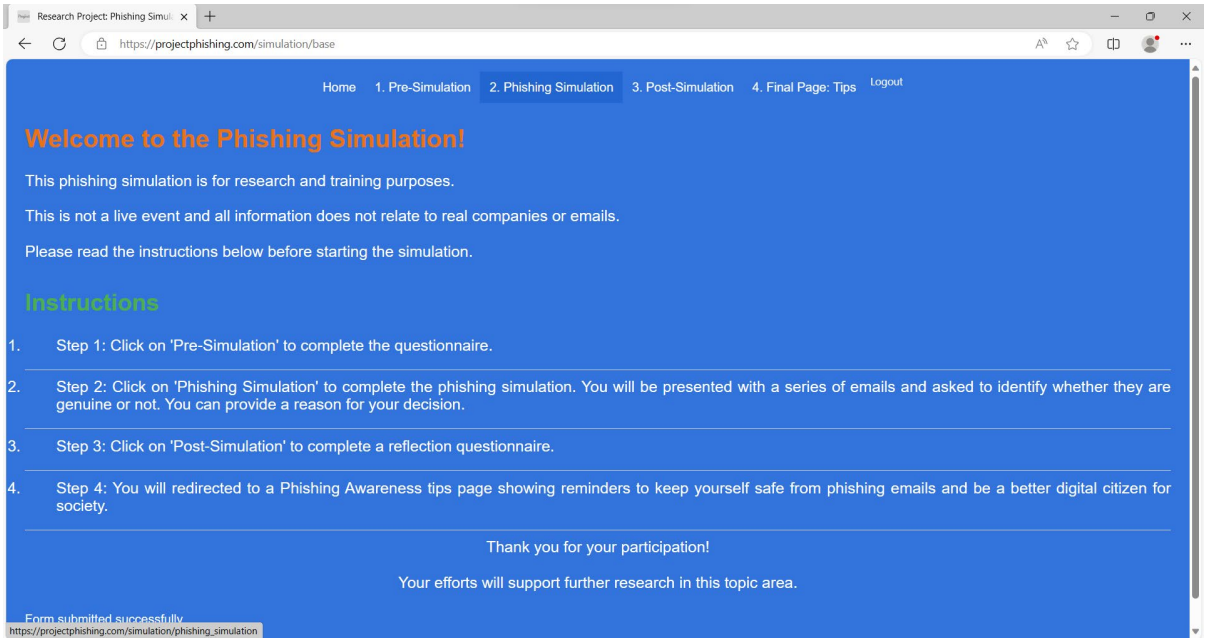


Figure 13: Base page prior to phishing simulation

```python
def calculate_score(user_id):
    # Fetch all responses for the given user_id
    responses = PhishingResponse.query.filter_by(user_id=user_id).all()

    # Initialize score
    total_score = 0

    # Weights for different aspects
    correctness_weight = 0.5      You, 2 weeks ago • simulation views
    confidence_weight = 0.3
    time_weight = 0.2

    for response in responses:
        # Initialize individual_score
        individual_score = 0

        # Fetch the corresponding challenge
        challenge = PhishingChallenge.query.get(response.challenge_id)

        # Correctness
        correct_answer = "phishing" if challenge.is_phishing else "genuine"

        if response.phishing == correct_answer:
            individual_score += correctness_weight * 100
        elif response.phishing == "unsure":
            individual_score += correctness_weight * 50
        else:
            individual_score += 0

        # Confidence
        if response.confidence == "high":
            individual_score += confidence_weight * 100
        elif response.confidence == "medium":
            individual_score += confidence_weight * 60
        else:  # Assuming 'low' is the only other option
            individual_score += confidence_weight * 30

        # Time
        time_score = 100 - (response.duration / 60 * 100)
        time_score = max(0, time_score)
        individual_score += time_weight * time_score

        total_score += individual_score

    if len(responses) > 0:
        average_score = total_score / len(responses)
    else:
        average_score = 0

    return average_score
```

Figure 14: Calculating user score in email challenges

Once the participant clicked on '2. Phishing Simulation' they were presented with one of the six spear phishing email challenges (Figure 16). The timer would begin when the page loaded, and participants could view, make decisions and provide feedback. To consider an adequate time for students to decide based on the email information, research was carried out by exploring the CEM Midyis, Yellis and Alis cognitive ability tests (Cambridge CEM, 2023) already undertaken by the students in the school. The overall non-verbal scores and cognitive

response times were considered to gauge a fair time for perception, processing and response. The processing time for participants' reading comprehension and process was considered, estimating 15 seconds to read the email challenge and 15 seconds to process and make decisions, aiming for an optimal 30-second duration. The maximum time the participant was allowed before the score became zero was 60 seconds (Figure 15).

```
def calculate_time_score(time_seconds):
    max_time = 60  # Maximum time in seconds after which the score becomes zero

    if time_seconds > max_time:
        return 0
    optimal_time = 30  # Optimal time in seconds to take for the decision 5 seconds and the typing time for the reason.
    time_penalty = (
        0.5  # Score reduction for each second above or below the optimal time
    )

    # The score starts at 10 and decreases by time_penalty for each second above or below the optimal time
    score = 10 - time_penalty * abs(optimal_time - time_seconds)

    # Make sure the score is within the bounds [0, 10]
    return max(0, min(10, score))
```

Figure 15: Calculating time

Processing times in education have been widely documented. Teachers are encouraged to provide 15 seconds of response time after reading for open-ended tasks (Hindman et al., 2019). Participants started with a score of 10, and the score was deducted 0.5 points per second on either side of the optimal time as participants may be impulsive or over-cautious, taking too long to decide. The dual process theory, one fast and one slow way of thinking (Kyllonen & Zu, 2016), can typically suggest that expert users automatically make a decision and will be faster compared to novices who take more time. This theory has been challenged as experts or perceived experts make errors through cognitive bias, such as confidence and higher ability users may not reconsider other aspects when processing (Wang & Xu, 2015) and that waiting time is more important than processing time to correlate cognitive ability (Schmiedek et al., 2007).

The 'Click this link' buttons allow participants to decide whether to click the link. This did not affect the simulation itself but was recorded in the database, and a flash message would indicate if they clicked on the link. The aim was to see if participants were happy to click on the link, if they decided the email was genuine or if they clicked the link regardless.

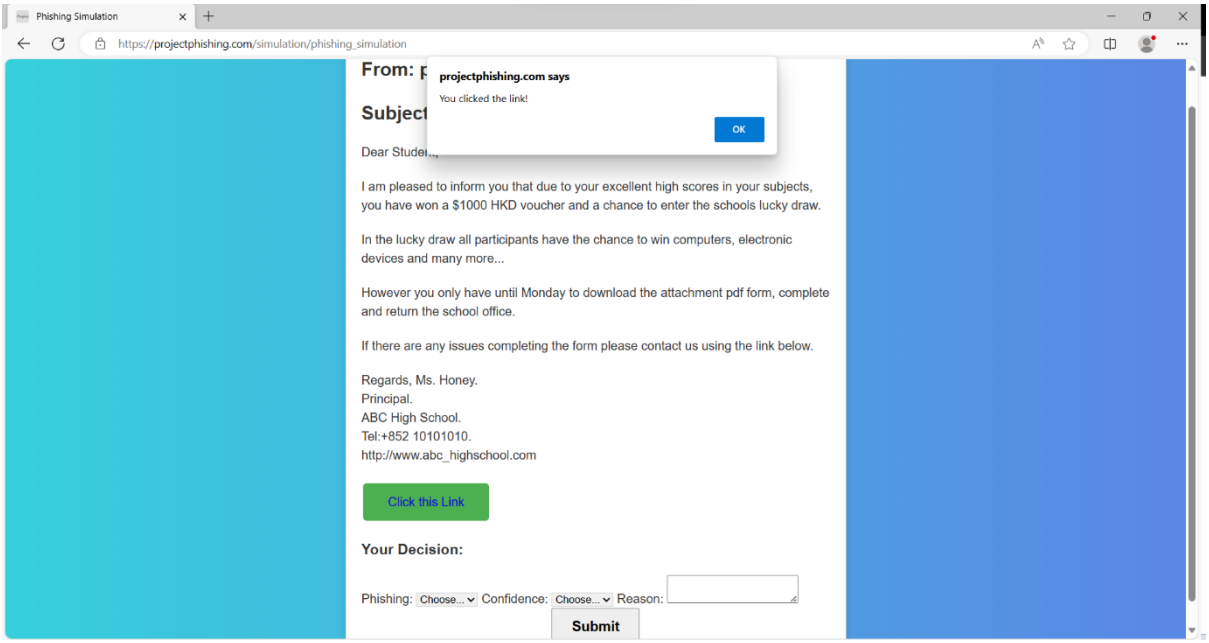


Figure 16: Example phishing email challenge

Email decisions are selected using the drop-down menu 'Genuine', 'Phishing' or 'Unsure' (Figure 17). Students are accustomed to completing electronic forms and have sufficient fine motor skills to manage and navigate the application forms. Scoring was applied here for the correct guess, gaining 50% of the score attributed. The participant could also rate how confident they were in the decision 'Low', 'Medium' or 'High', which provided 30% of the score for the challenge.

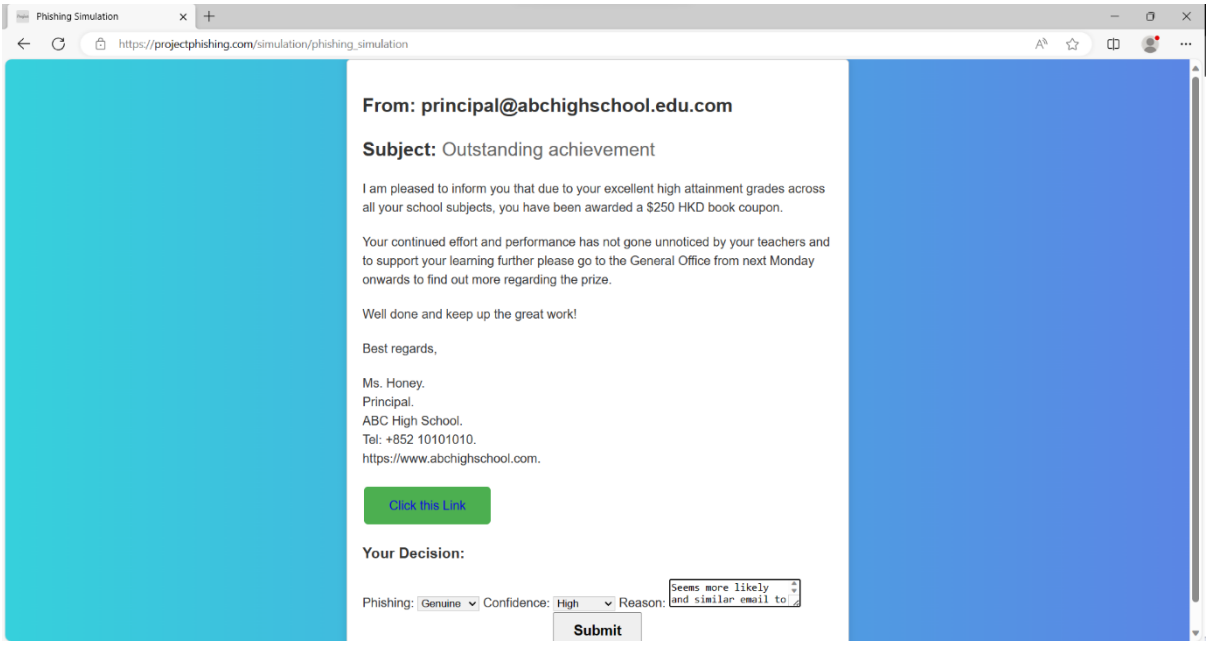


Figure 17: Example of genuine email with data input

The phishing email challenges (Figure 18, Figure 19) aligned with the research design, providing cues, and the context was related to the school's usual communications.

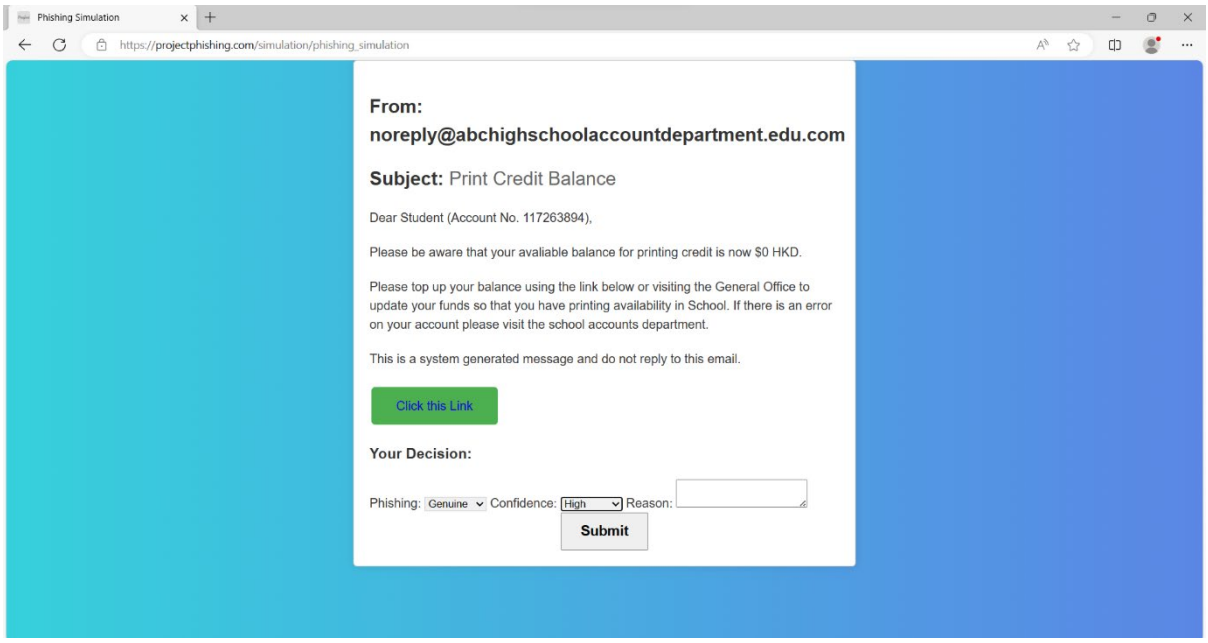


Figure 18: Example email challenge

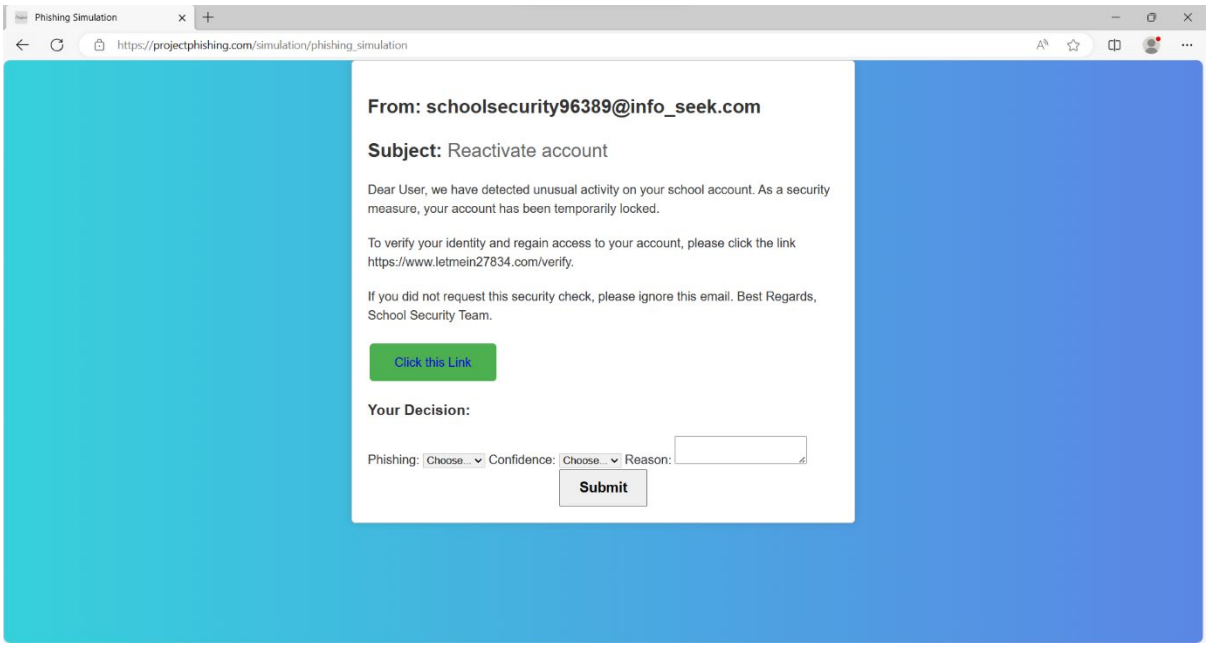


Figure 19: Example of phishing email for cue identification

Participants were redirected back to the base page after completing six email challenges before being instructed to complete '3. Post Simulation'. The questionnaire reflected on the simulation and consolidated knowledge of cyber awareness behaviours (Figure 20, Figure 21).

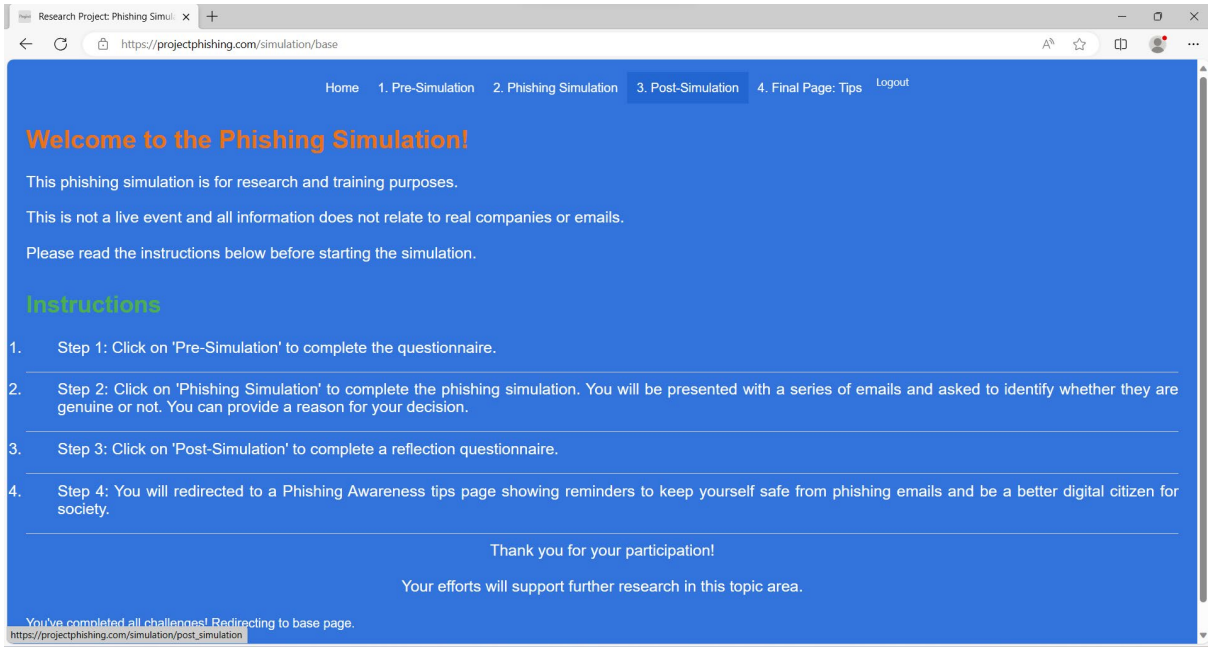


Figure 20: Base page

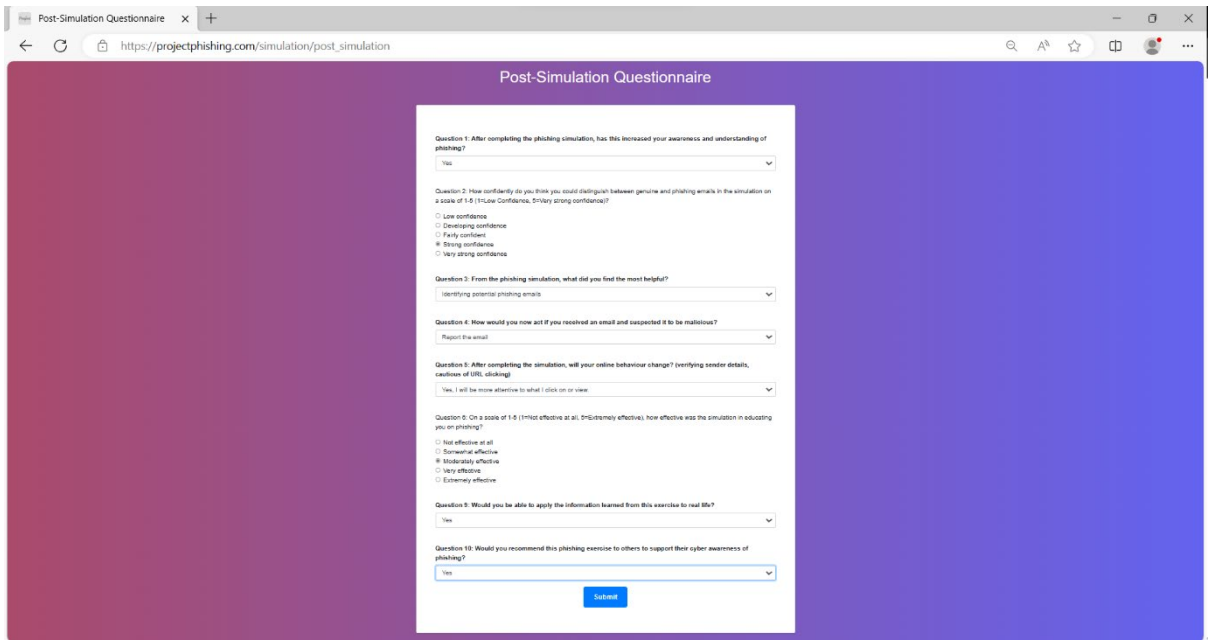


Figure 21: Post-Simulation Questionnaire

Participants were redirected to a final page showing results (Figure 22). The overall score was a combined score from all the email challenges (Figure 23), which was aligned against a grade-level boundary (Figure 24).

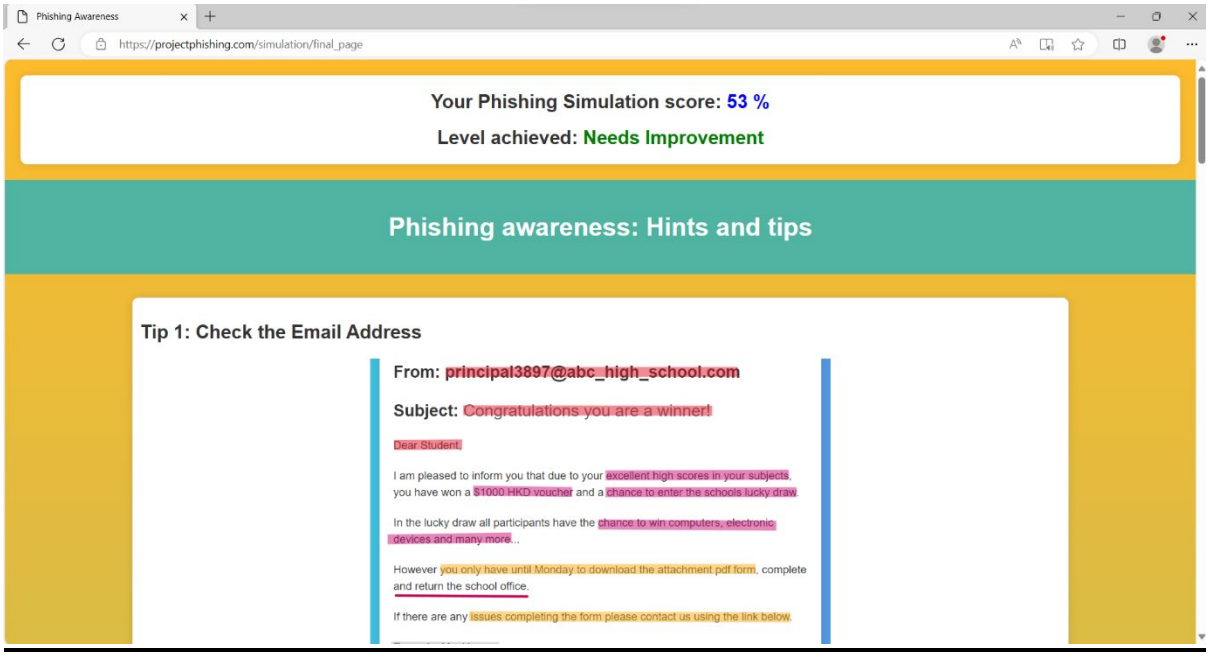


Figure 22: Final page showing the overall user score and grade level

```python
@simulation_blueprint.route("/final_page")
@login_required
def final_page():
    # Calculate the score and grade using the function
    average_score, grade = calculate_score_and_grade(current_user.id)

    # Round the score
    rounded_score = round(average_score)

    # Pass the calculated score and grade to the HTML template
    return render_template(
        "simulation/final_page.html", user_score=rounded_score, grade_level=grade
    )
```

Figure 23: Calculating overall score and grade for the final page

```python
def calculate_score_and_grade(user_id):
    average_score = calculate_score(
        user_id
    )  # Assuming calculate_score is defined as before

    # Determine grade
    if average_score >= 90:
        grade = "Excellent"
    elif average_score >= 80:
        grade = "Very Good"
    elif average_score >= 70:
        grade = "Good"
    elif average_score >= 60:
        grade = "Fair"
    elif average_score >= 50:
        grade = "Needs Improvement"
    else:
        grade = "Poor"

    return average_score, grade
```

Figure 24: Calculating overall score and grade level

The final page also allows participants to review their progress and evaluate their performance in the simulation. Each email challenge is shown again with highlighted colours to identify the cue with justification noted below each email, identifying whether the email was genuine or phishing (Figure 25, Figure 26, Figure 27). Participants cannot view this information unless they have completed the previous steps.

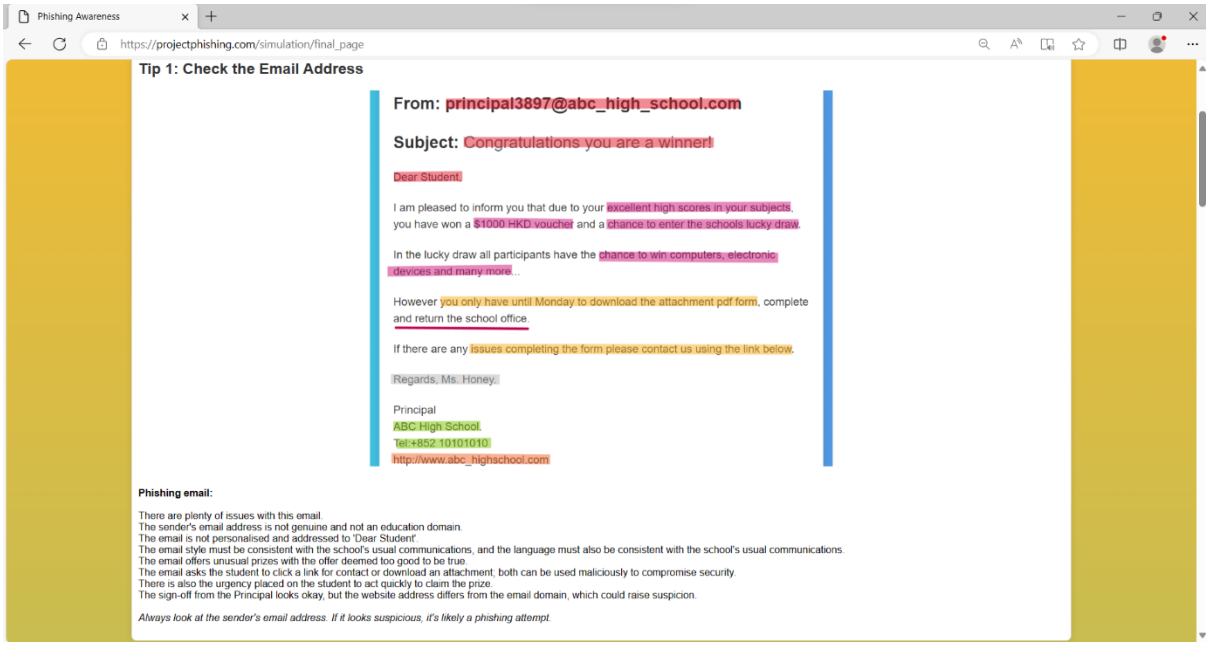


Figure 25: Final page cue identification and cyber awareness tips

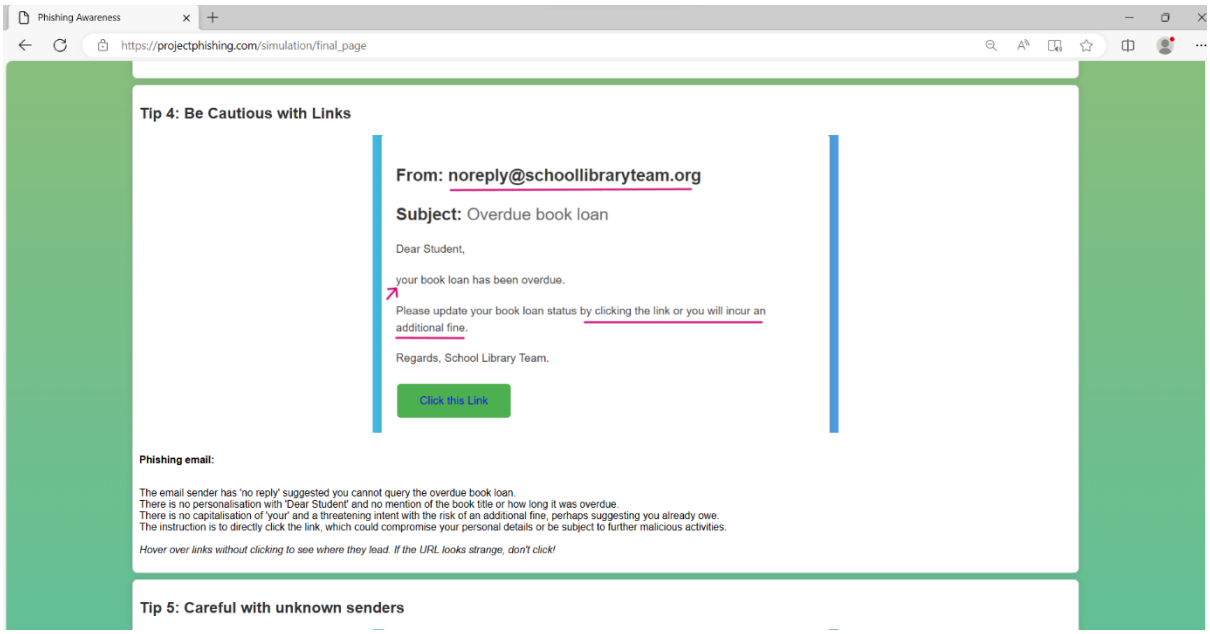


Figure 26: Example of a phishing email with fewer cues

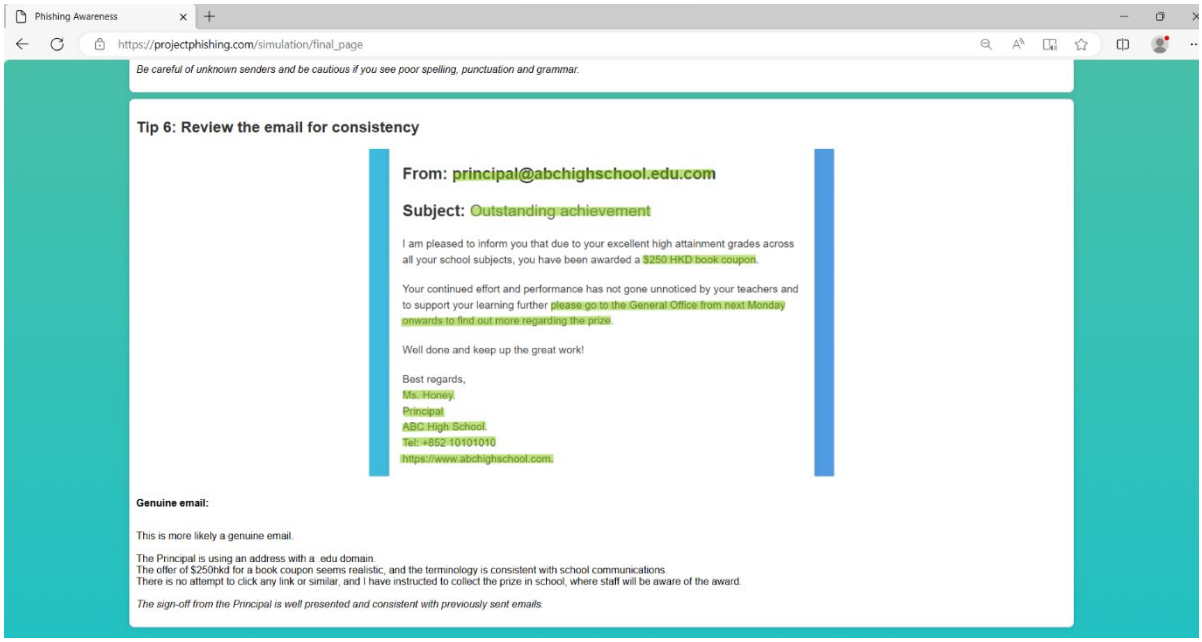


Figure 27: Example of genuine email identifying cues

4.2.4 Data collection

The data was collected via the web application designed using the Python Flask framework with a cloud-based database third-party provider. Ensuring all participants' interactions were logged with appropriate security measures is essential to ensure the data's confidentiality, integrity, reliability, availability and compliance with the CIA triad (Ham, 2021). Furthermore, utilising and complying with the Open Web Application Security Project (OWASP) Top 10 document (OWASP, 2023) offered awareness of security risks and measures to prevent them. By aligning with the guiding principles, the web application reduces risk and enhances trust and a positive approach to reliability (Fredj et al., 2021).

Following registration, the data collected from participants was limited to username, age, and gender, with universally unique identifiers (UUIDs) used as primary keys in the database table to offer enhanced privacy (Das et al., 2020).

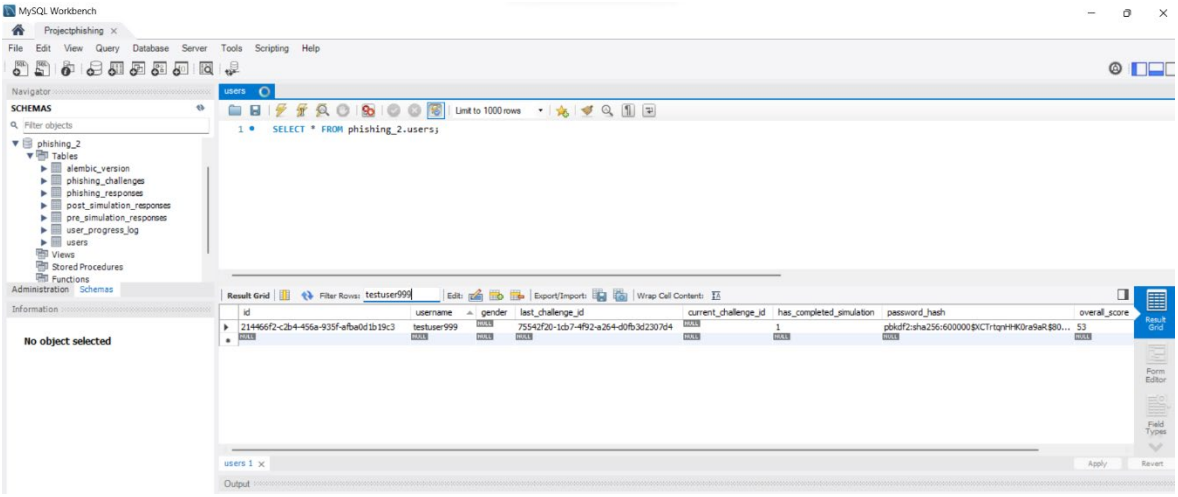


Figure 28: User profile in the database

The werkzeug.security library provides password hashing before database storage, enhancing security against reverse engineering and increasing user trust (Rayhan et al., N.D.). Password validation offers increased security against unauthorised access. SQLAlchemy object-relational mapping (ORM) shields data integrity and prevents SQL injection attacks, whilst flask_login manages authentication and user sessions through flask_session and greater flexibility in storing session data on the client or server sides. Registration checks to prevent duplication Appendix 16 and flash messages are issued for users' actions. If registration errors occur, the try-except block handles this and rolls back the transaction (Figure 29).

```python
@bp.route('/register', methods=['GET', 'POST'])
def register():
    logging.info("Register route hit")
    username = request.form.get('username')
    logging.debug(f"Attempting to register username: {username}")
    form = RegistrationForm()
    if form.validate_on_submit():
        username = form.username.data
        password = form.password.data

        user_exists = User.query.filter_by(username=username).first()

        if user_exists:
            flash('Username already exists. Please choose a different one.')
            return redirect(url_for('auth.register'))

        try:
            user = User(username=username, password=password)
            db.session.add(user)
            db.session.commit()

            flash('Your account has been created! You can now login.')
            return redirect(url_for('auth.login'))
        except Exception as e:
            db.session.rollback()  # Rollback the transaction on error
            flash('An error occurred during registration. Please try again later.')
            return redirect(url_for('auth.register'))

    logging.info("Finished registration process")
    return render_template('auth/register.html', form=form)
```

Figure 29: Registration route

Further error handlers (Figure 30) are defined for HTTP status codes 400, 403, 404 and 500 to support user experience with customised communication and support development to identify errors for troubleshooting.

```python
# Error handlers
@simulation_blueprint.app_errorhandler(500)
def internal_server_error(e):
    current_app.logger.error(f"Internal Server Error: {e}")
    return render_template("500.html"), 500


@simulation_blueprint.app_errorhandler(404)
def not_found_error(e):
    current_app.logger.error(f"404 Error: {e}")
    return render_template("404.html"), 404


@simulation_blueprint.app_errorhandler(403)
def forbidden_error(e):
    current_app.logger.error(f"403 Error: {e}")
    return render_template("403.html"), 403


@simulation_blueprint.app_errorhandler(400)
def bad_request(e):
    current_app.logger.error(f"400 Error: {e}")
    return render_template("400.html", error=e), 400
```

Figure 30: Error handlers

Users will enjoy a secure experience as only authenticated users can access the simulation, and unauthorised access will be prevented after password verification. The application also supports safe redirection in Figure 31 for the 'next' argument, which cannot be a vulnerability preventing open redirection attacks.

```python
@bp.route('/login', methods=['GET', 'POST'])
def login():
    if current_user and current_user.is_authenticated:
        return redirect(url_for('simulation.base'))
    form = LoginForm()
    if form.validate_on_submit():
        user = User.query.filter_by(username=form.username.data).first()
        if user is None or not user.check_password(form.password.data):
            flash('Invalid username or password')
            return redirect(url_for('auth.login'))
        login_user(user, remember=form.remember_me.data)
        next_page = request.args.get('next')
        if not next_page or url_parse(next_page).netloc != '':
            next_page = url_for('simulation.base')
        return redirect(next_page)
    return render_template('auth/login.html', title='Sign In', form=form)
```

Figure 31: Login route

The flash messages improve communication to the user, and errors are handled to ease the user experience whilst the messages are rendered through flask templating Jinja2. Flask_wtf allows

Cross-Site Forgery Protection (CSRF) (Figure 32) to support genuine form submission requests, enhancing trust in the application. Cross-site scripting attacks (XSS) are further protected against utilising Jinja2 templating in HTML pages to mitigate data rendering (Song, 2022).

```python
def create_app(config_name=None):
    app = Flask(__name__)
    csrf = CSRFProtect()
    if config_name == "testing":
        app.config.from_object('my_app.config.TestingConfig')
    elif os.environ.get('FLASK_ENV') == 'production':
        app.config.from_object('my_app.config.ProductionConfig')
    else:
        app.config.from_object('my_app.config.DevelopmentConfig')
    Session(app)
    configure_logging(app)
    db.init_app(app)
    login_manager.init_app(app)
    csrf.init_app(app)
    migrate.init_app(app, db)
```

Figure 32: __init__.py CSRF Protection

Loading environment variables with the dotenv library separates sensitive configuration from the codebase. Rotating file handlers in logging ensures monitored activities are traceable for review. Additionally, access control restricts access to endpoints such as the 'final page' (Figure 33), permitting only users who have completed the previous steps.

```python
@login_manager.user_loader
def load_user(user_id):
    return User.query.get(str(user_id))

from .main import bp as main_bp
from .auth import bp as auth_bp

app.register_blueprint(auth_bp, url_prefix='/auth')
app.register_blueprint(main_bp)
app.register_blueprint(simulation_blueprint, url_prefix='/simulation')
app.cli.add_command(seed_database)


@app.before_request
def restrict_access():
    if request.endpoint == 'simulation.final_page' and not current_user.has_completed_simulation:
        return redirect(url_for('simulation.base'))


@app.route('/simulation/final_page')
def show_final_page():
    return render_template('simulation/final_page.html')

return app
```

Figure 33: __init__.py before_request access control

Hypertext Transfer Protocol Secure (HTTPS) certification (Figure 34) encrypts data between the user's browser and server, ensuring integrity and mitigating man-in-the-middle attacks that could compromise sensitive information (Ghimire, 2020). It enhances cookie security, reducing session hijacking risk by transmitting cookies only over HTTPS. The padlock icon in the browser symbolises trust and credibility, preventing warning messages that could deter users.

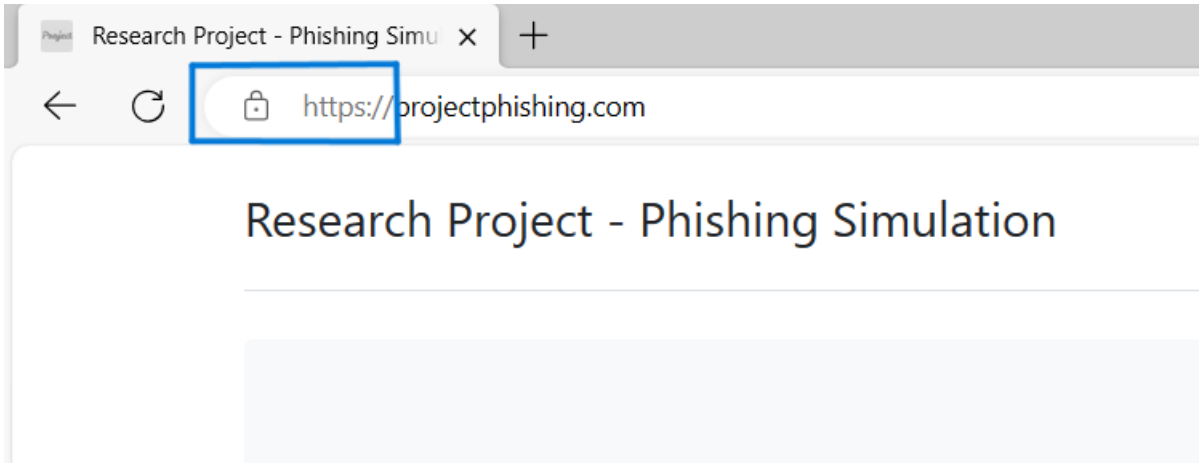


Figure 34: Use of HTTP

Hosted by a third-party cloud provider, the database ensures data integrity with backup and recovery mechanisms. Provider selection was critical for ensuring continuous access and scalability under heavy user load. The low participation turnout could not have been anticipated prior to data collection, so a cloud database offering high availability maintenance with security updates offers a cost-effective and reliable solution to build user trust. The simulation yielded valuable insights, capturing data on phishing email detection accuracy, response times, URL click behaviours, decision-making confidence, and reasoning (Figure 35).

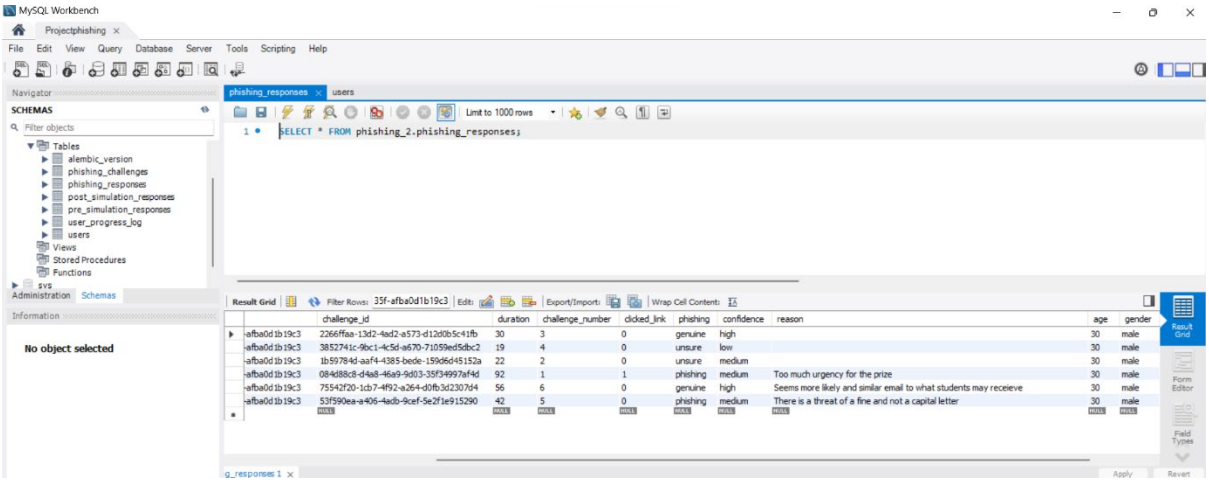


Figure 35: Test user data collected phishing responses

Quantitative and qualitative data were gathered from pre and post-simulation questionnaires. Participants' age and gender (Figure 36, Figure 37) informed analyses to avoid replication and a better user experience. The process was conducted silently to eradicate discussions affecting decisions or judgements between participants.

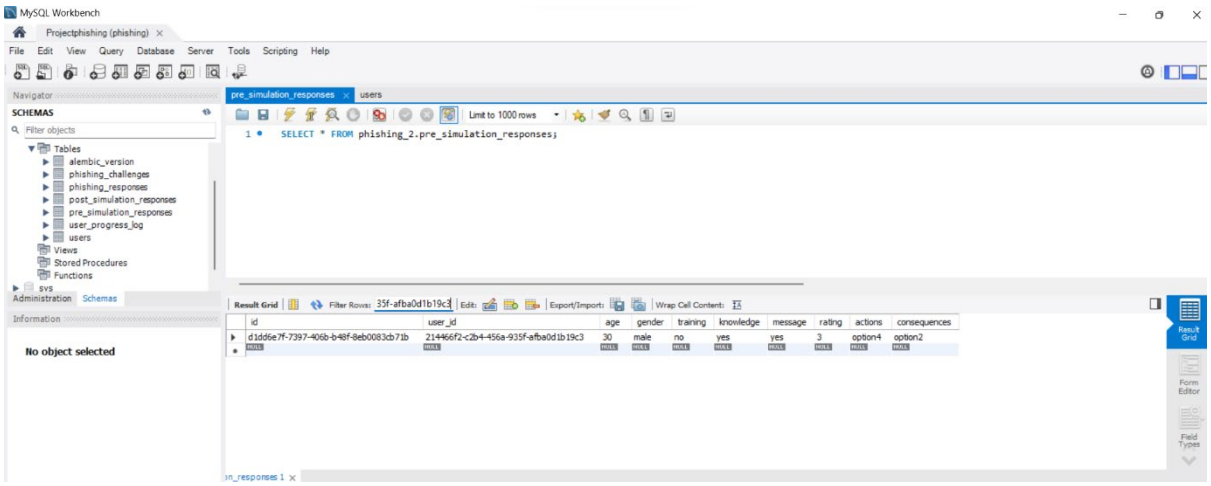


Figure 36: User responses from the Pre-Simulation Questionnaire

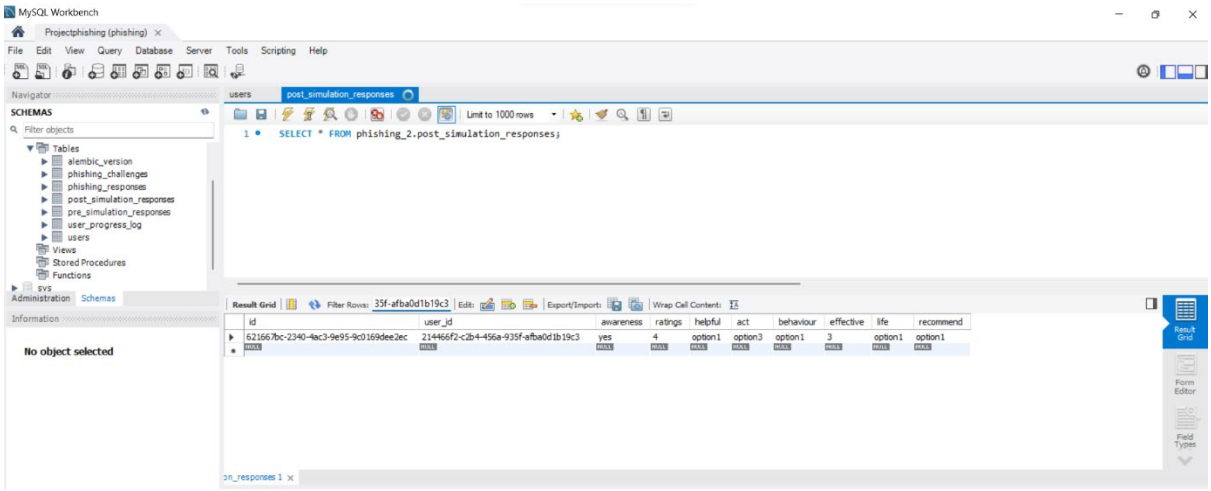


Figure 37: User responses from the Post-Simulation Questionnaire

The artefact was tested using Pytest and Unittest. The summary of tests is found in Appendix 15; examples of the test cases can be found in Appendix 16 and Appendix 17. The code was also tested with Pylint (Examples in Appendix 18, Appendix 19) and Flake 8 (Appendix 20) for error checking in code and applying PEP8 standards.

4.3 Data Analysis (2413 words)

The main objective of the data analysis aimed to find insights into the students' efficacy in using cybersecurity awareness to empower them to mitigate phishing attempts.

4.3.1 Descriptive statistics

Prior to the phishing simulation

Table 2: Descriptive analysis of participants' age and overall score in the phishing simulation

Participants	46	
Statistic	**Age**	**Overall Score**
Mean (Average)	15.7	53.7
Standard Deviation	1.2	9.6
Minimum	13	35
Maximum	18	70
Range	5	35
25th Percentile	15	
50th Percentile	16	
75th Percentile	16.75	

Demographic analysis revealed an average age of 15.7 years, ranging from 13 to 18. Figure 39 shows that 25% of the sample were 15 or younger, 50% were 16 or younger, and 75% were no older than 16.75 years.

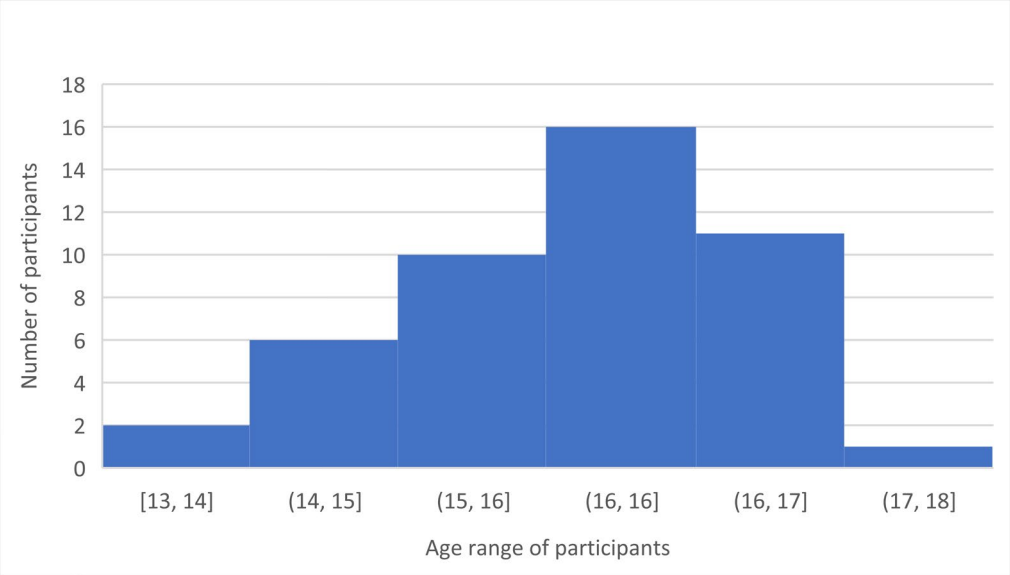


Figure 38: Histogram to show the age distribution of participants

The highest number of participants were aged between 15 and 17 years.

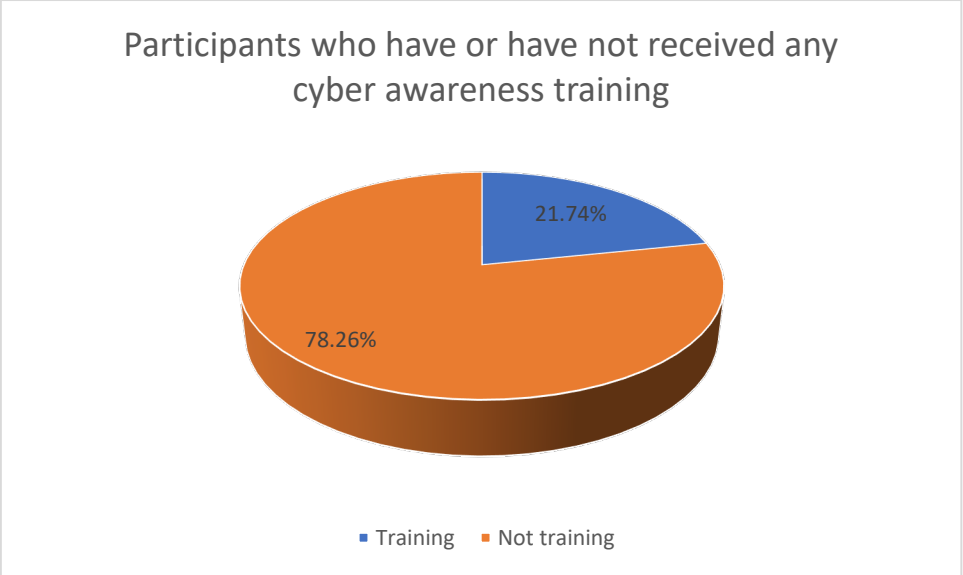


Figure 39: Participants response regarding cyber awareness training

Most participants responded by saying they had not received any cyber awareness training.

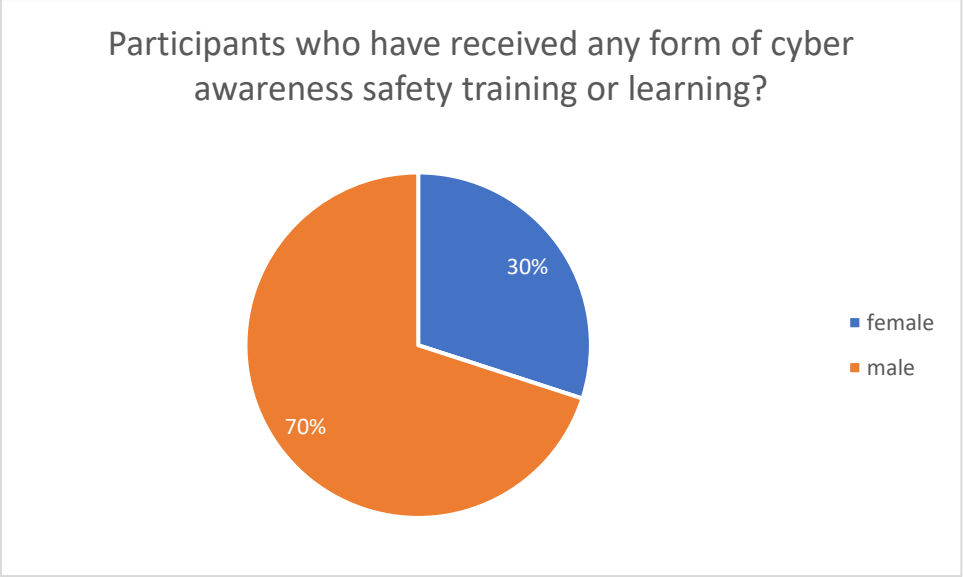


Figure 40: Gender ratio for participants who have received any form of cyber awareness training

For the 21.74% of participants who had received cyber awareness training, males were the majority compared to females.

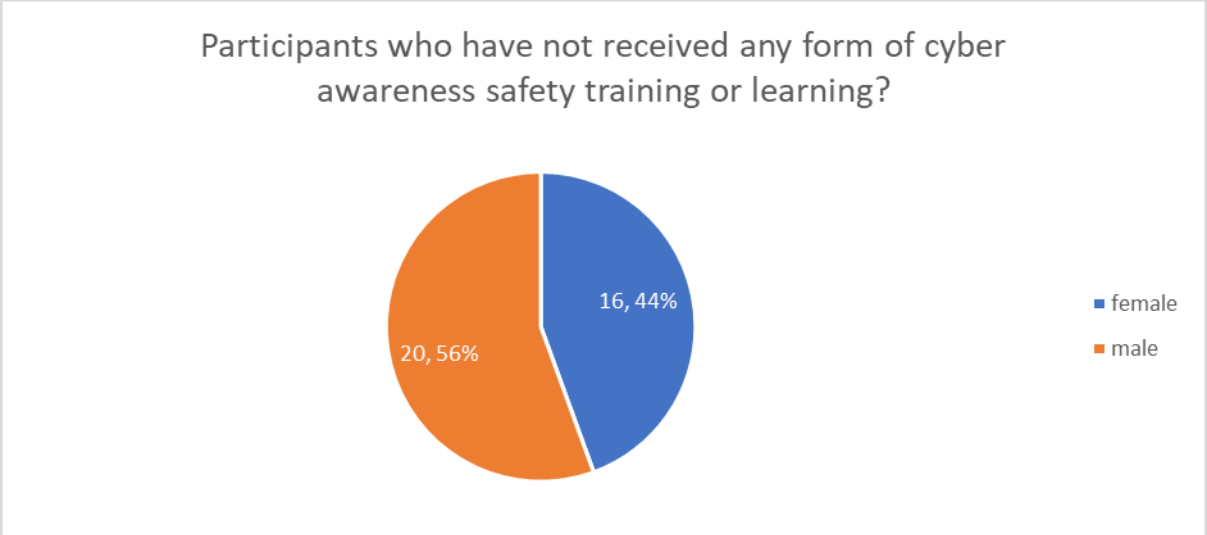


Figure 41: Participants who have not received any cyber awareness training based on gender

For the 78.26% of those who indicated they had not received training, the gender gap was closer with males at 56%.

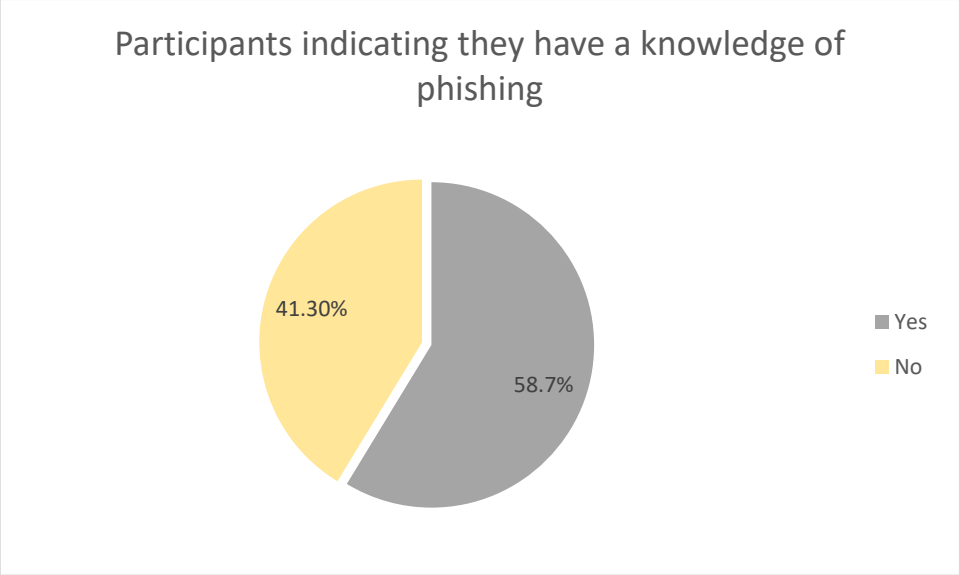


Figure 42: Participants with knowledge of phishing from the pre-questionnaire

However, despite only 21.74% suggesting they had trained previously, 58.7% of all participants indicated they knew about phishing.

Figure 43: Participants indicated they had received a suspected phishing attempt in the pre-questionnaire.

Most participants indicated they had received a suspected phishing attempt, which could support the phishing knowledge.

Table 3: Confidence in distinguishing genuine and phishing emails

Metric	Overall gender	Male	Female
Average confidence level	2.87	2.96	2.74
Standard deviation	0.99	1.10	0.78
Minimum confidence level	1	1	1
Maximum confidence level	5	5	4

There is a slight difference in confidence levels in favour of males and females. No female rated her confidence as the maximum level.

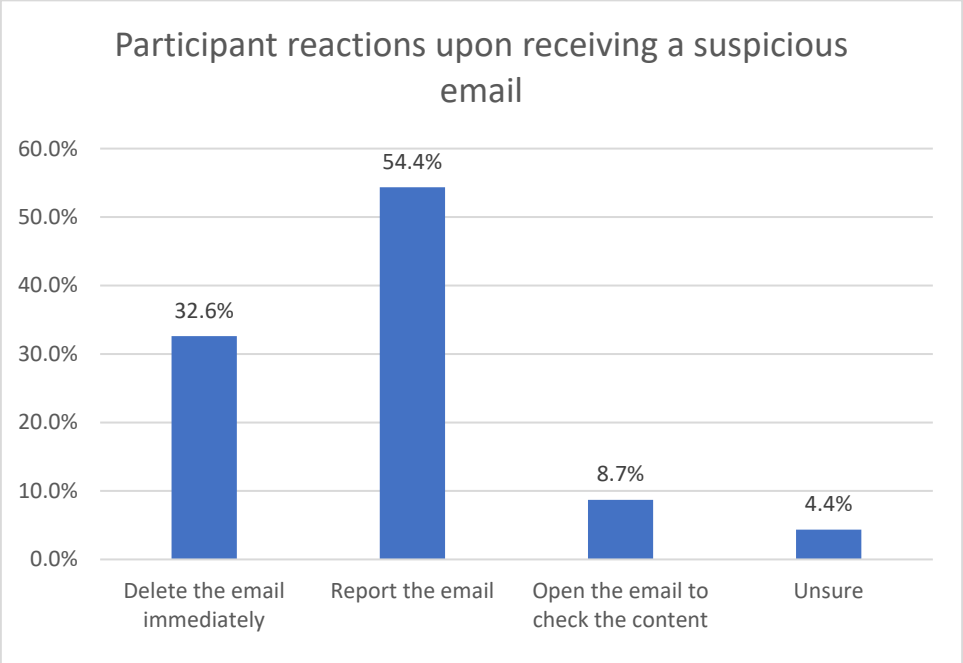


Figure 44: Participants reactions upon receiving a suspicious email

Phishing simulation:

Table 4: Rank and percentile of overall scores based on gender

Point	*male*	*Rank*	*Per cent*	*Point*	*female*	*Rank*	*Per cent*
11	70	1	96.1%	14	68	1	100.0%
18	70	1	96.1%	7	65	2	94.4%
4	67	3	92.3%	5	64	3	83.3%
24	65	4	88.4%	15	64	3	83.3%
10	64	5	84.6%	19	62	5	77.7%
1	61	6	76.9%	9	61	6	66.6%
15	61	6	76.9%	10	61	6	66.6%
20	59	8	73.0%	16	56	8	61.1%
7	57	9	61.5%	2	55	9	50.0%
12	57	9	61.5%	17	55	9	50.0%
26	57	9	61.5%	8	54	11	38.8%
5	56	12	57.6%	13	54	11	38.8%
13	54	13	50.0%	11	53	13	33.3%
23	54	13	50.0%	12	52	14	27.7%
2	53	15	42.3%	1	50	15	22.2%
6	53	15	42.3%	4	44	16	16.6%
9	52	17	34.6%	3	40	17	11.1%
16	52	17	34.6%	6	39	18	5.5%
19	51	19	30.7%	18	37	19	0.0%
14	49	20	26.9%	20		#N/A	#N/A
3	47	21	23.0%	21		#N/A	#N/A
8	42	22	19.2%	22		#N/A	#N/A
22	40	23	15.3%	23		#N/A	#N/A
21	38	24	11.5%	24		#N/A	#N/A
17	37	25	3.8%	25		#N/A	#N/A
25	37	25	3.8%	26		#N/A	#N/A
27	35	27	0.0%	27		#N/A	#N/A

The table identifies the scores between males and females and phishing identification ability. The top score of 70 suggests a good level of phishing awareness, but below 50 was graded as a poor level. The majority of participants were graded as fair.

Table 5: Show the overall accuracy per email challenge

Email Challenge	Count	Correctly guessed	Percentage	Type:
Challenge 1	46	35	76%	Phishing
Challenge 2	46	25	54%	Phishing
Challenge 3	46	30	65%	Genuine
Challenge 4	46	31	67%	Phishing
Challenge 5	46	21	46%	Phishing
Challenge 6	46	45	98%	Genuine

The analysis identifies the participant's accuracy scores per email challenge.

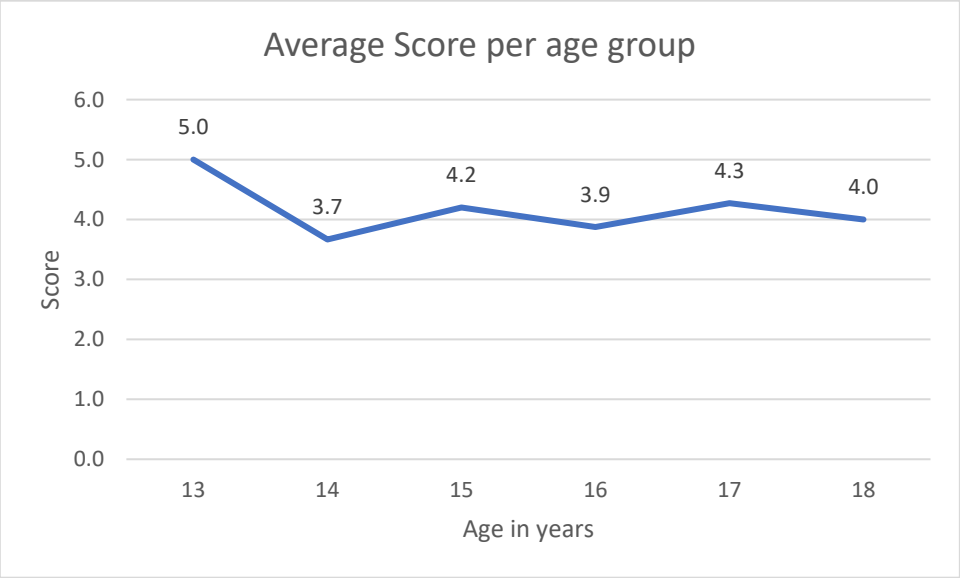


Figure 45: Average score per user from 13-18 year olds

The chart identifies the average score per age group of participants. The youngest age group scored the highest score; however, there were only two participants in this age group. Overall, there were no significant differences between ages.

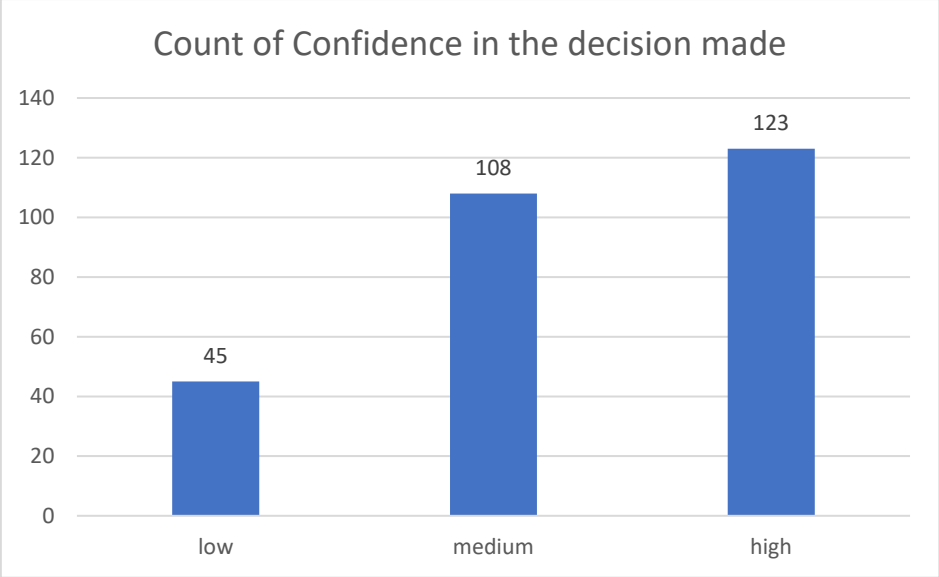


Figure 46: Participants confidence in their decision making

Most participants had high and medium confidence in their decision-making on identifying genuine or phishing emails.

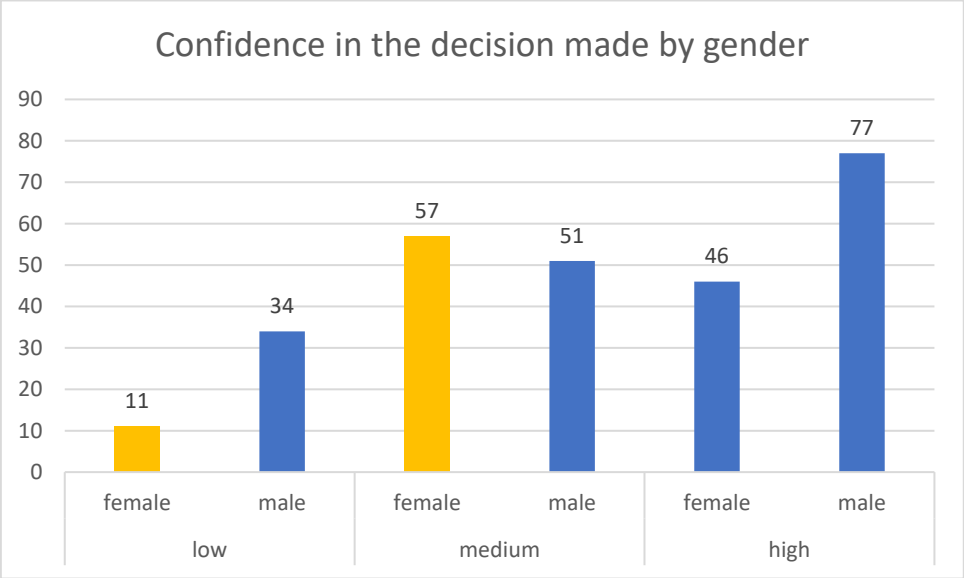


Figure 47: Participants confidence in their decision-making by gender

Concerning gender, more females were applying medium confidence to their decision-making, whilst most males had high confidence in their decision-making.

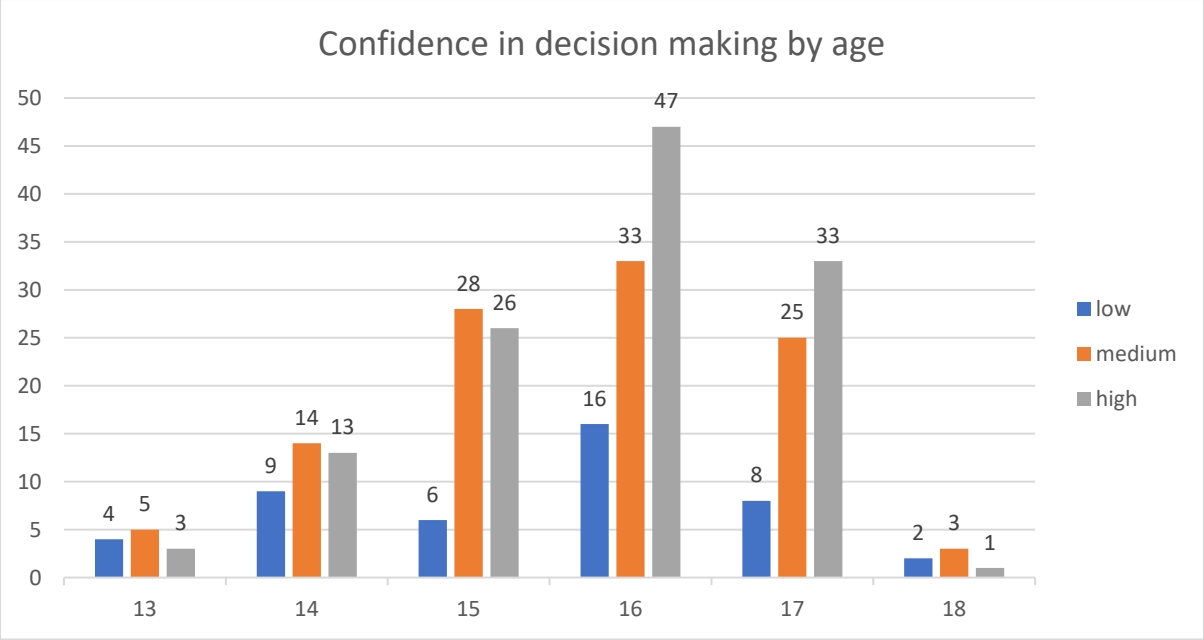


Figure 48: Participants confidence in their decision-making by age of both genders

Most students were between 15 and 17 years old, and this data suggests they were more confident in their decision-making.

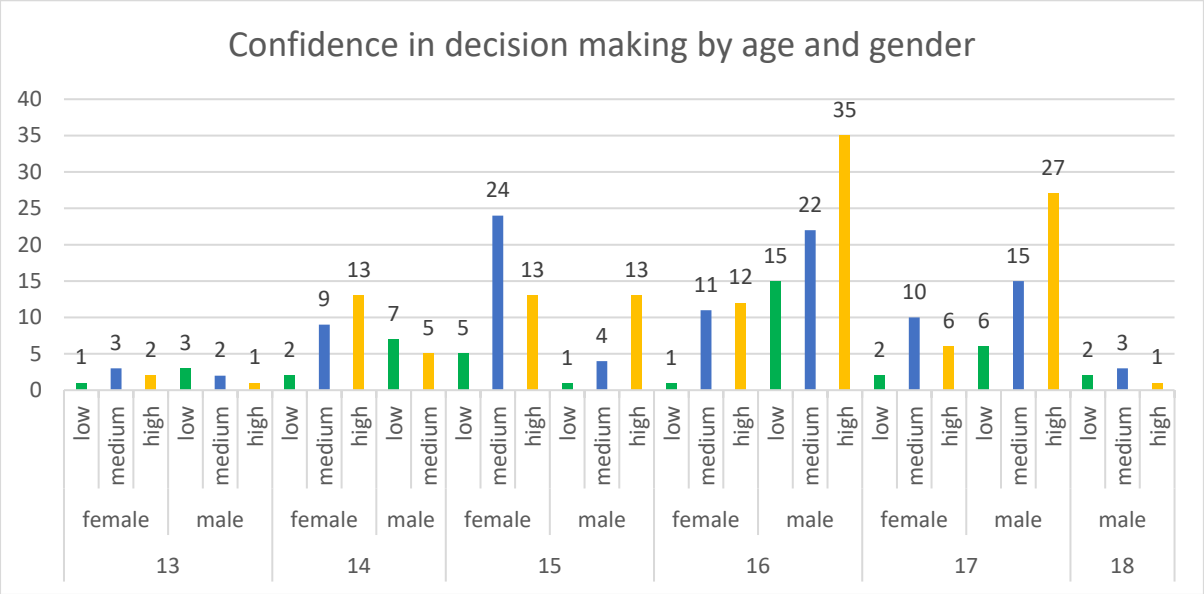


Figure 49: Participants' confidence in their decision-making by age and gender

Males tend to have a higher confidence level across age groups, with 16-17 year olds seeming to be more confident overall. This does tend to suggest a possible relationship that older participants are more confident.

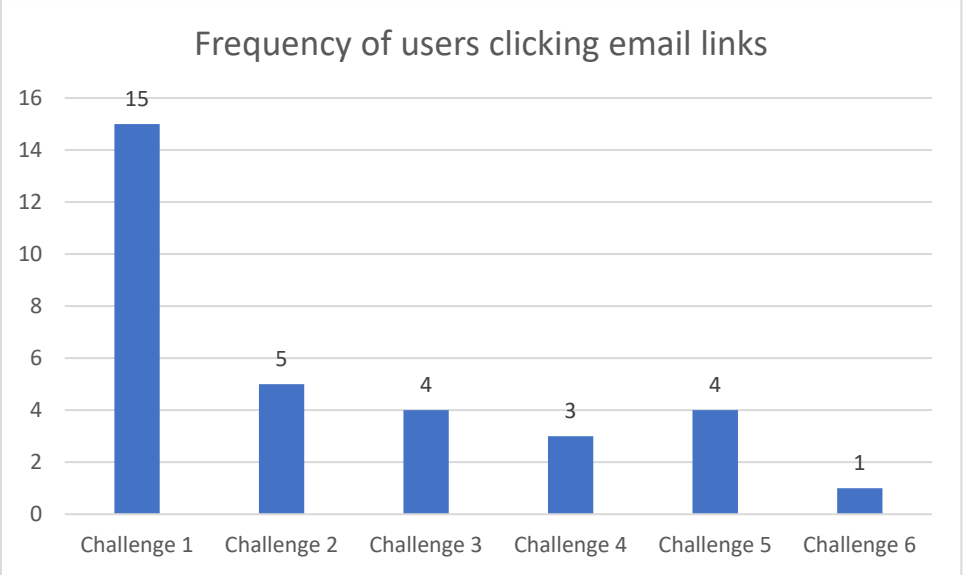


Figure 50: Participants frequency of clicking the URL links in the email challenges

Participants were keen to click Challenge 1 the most compared to the other challenges. In contrast, Challenge 6 was a genuine but similar type of email and only received one click.

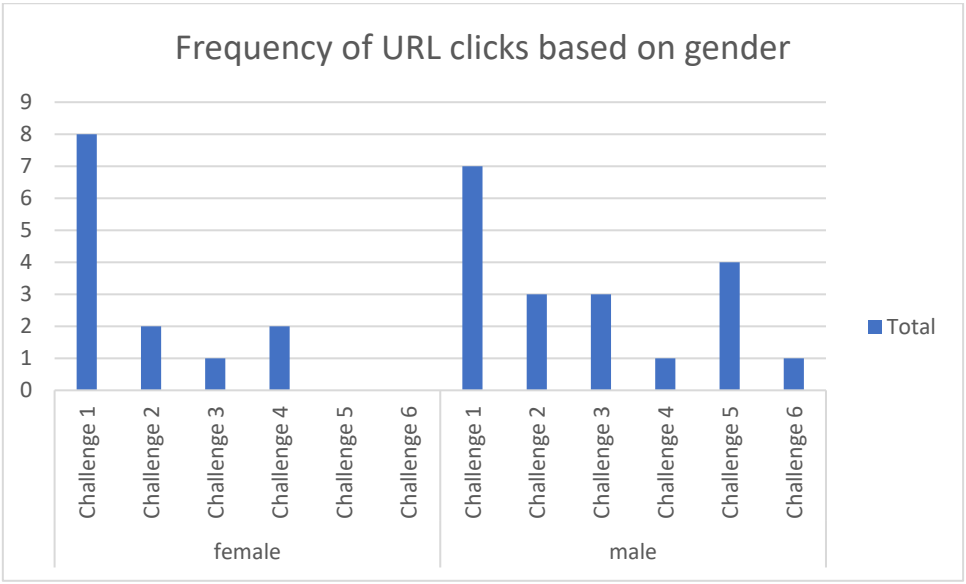


Figure 51: Participants' frequency of clicking the URL links in the email challenges by gender

Males incurred a more comprehensive number of clicks across all challenges, whereas females only clicked from 1 to 4. Males accumulated more clicks than females; the male average click rate was 10.91%, whereas the female average click rate was slightly higher, 12.74%.

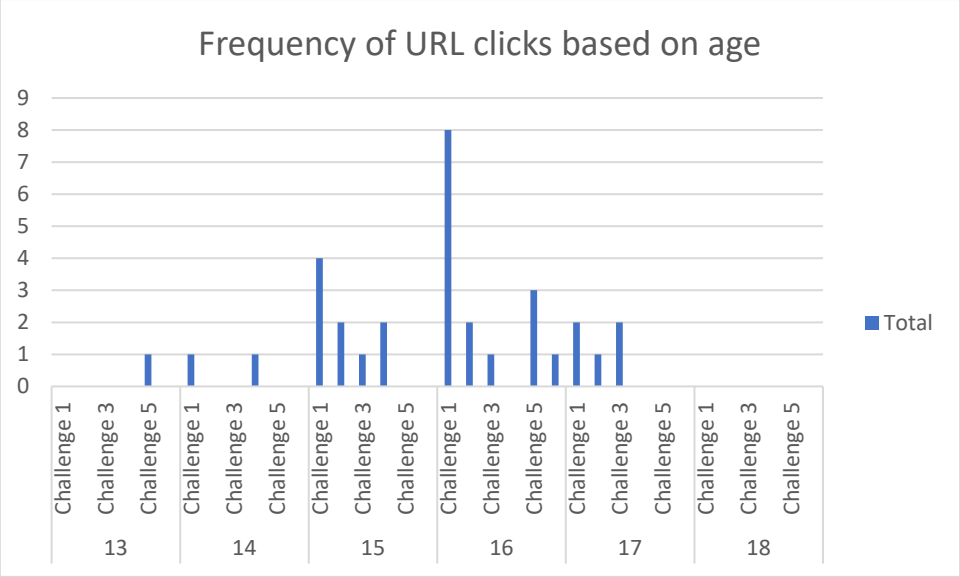


Figure 52 Participants frequency of clicking the URL links in the email challenges by age

Most clicks were in the 15-17-year age group; whilst this is in line with the participation uptake, it does not suggest any significant correlation or causation.

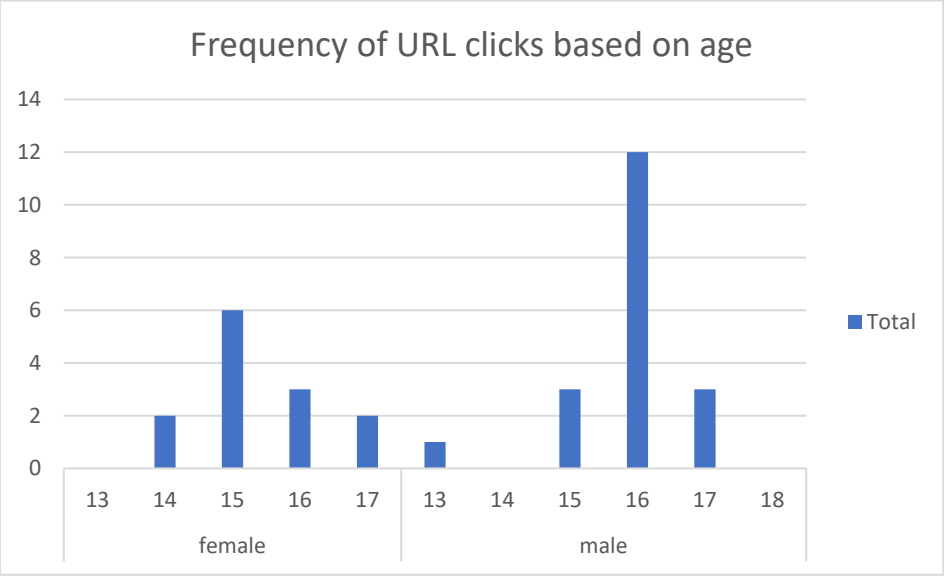


Figure 53: Click rates based on age by gender

The most common age for click rates was 16-year-olds for males and 15-year-olds for females.

After the phishing simulation:

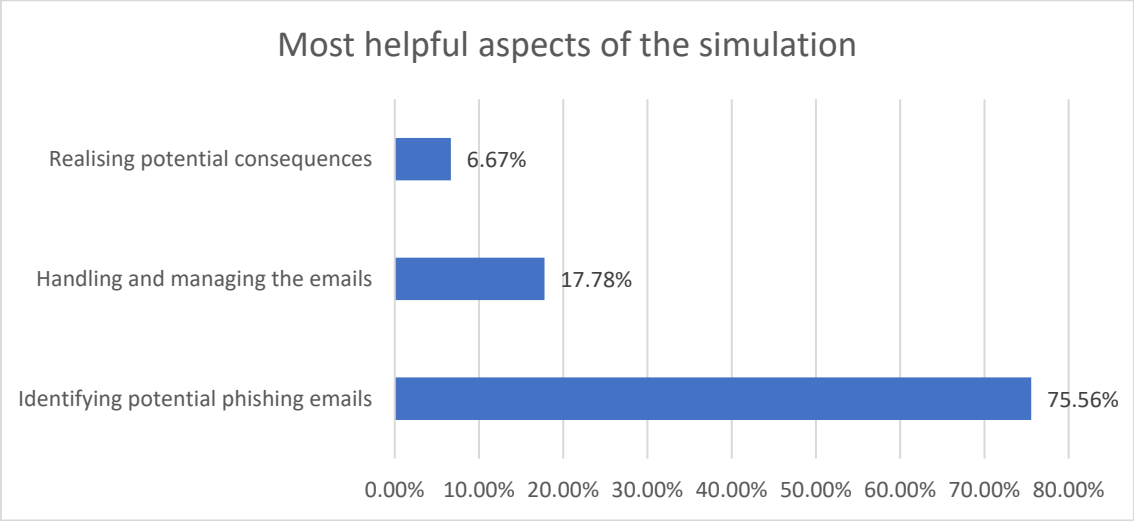


Figure 54: Participants identify the most helpful aspects of the simulation

Participants unanimously responded that identifying phishing emails was the most helpful aspect of the simulation.

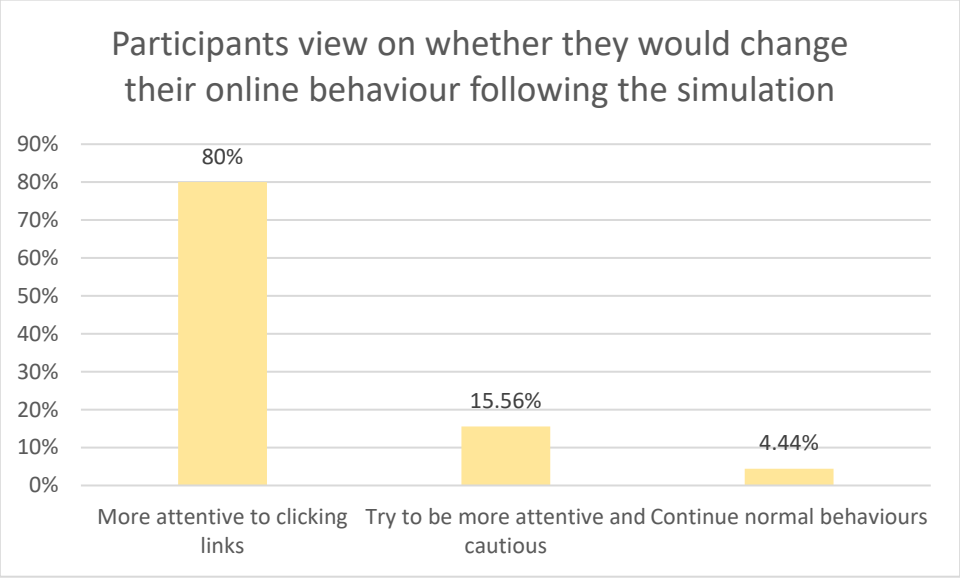


Figure 55: Participants suggesting if they would change their future online behaviours

Participants indicated that they would change their online behaviours due to the simulation, with nearly all being attentive to clicking links and others being more cautious when opening emails. A small percentage said they would continue with current practices.

Table 6: Rating the effectiveness of the phishing simulation in educating users

Statistic	Value
Mean (Average)	3.38
Standard Deviation	0.94
Minimum	1
Maximum	5
Median	4

Participants' mean score would suggest they found the simulation somewhat effective, which is a positive response, and suggests they found it beneficial to learning; however, some participants did not find it helpful.

4.3.2 In-depth analysis

Table 7: t-Test for the overall score for males and females

t-Test: Two-Sample Assuming Unequal Variances		
	Variable 1	*Variable 2*
Mean	53.3	54.4
Variance	102.7	84.0
Observations	27	19
Hypothesised Mean Difference	0	
df	41	
t Stat	-0.4	
P(T<=t) one-tail	0.3	
t Critical one-tail	1.7	
P(T<=t) two-tail	0.7	
t Critical two-tail	2.0	

Females have slightly higher mean scores than males; however, due to the slight difference, gender is not considered to impact the overall scores significantly.

Table 8: t-Test for overall scores and prior knowledge of phishing

t-Test: Two-Sample Assuming Unequal Variances		
	Variable 1	*Variable 2*
Mean	53.3	54.3
Variance	96.1	93.8
Observations	27	19
Hypothesised Mean Difference	0	
df	39	
t Stat	-0.3	
P(T<=t) one-tail	0.4	
t Critical one-tail	1.9	
P(T<=t) two-tail	0.7	
t Critical two-tail	2.0	

The average score of participants without prior knowledge of phishing is slightly higher than those who suggested they knew about phishing, but the difference is slight, so it would not be considered significant.

Table 9: t-Test for overall scores and gender

t-Test: Two-Sample Assuming Unequal Variances		
	Variable 1	*Variable 2*
Mean	53.3	54.4
Variance	102.7	84.0
Observations	27	19
Hypothesised Mean Difference	0	
df	41	
t Stat	-0.4	
P(T<=t) one-tail	0.3	
t Critical one-tail	1.7	
P(T<=t) two-tail	0.9	
t Critical two-tail	2.0	

The average score of females is slightly higher than males; however, the difference is negligible. We can assume gender does not significantly impact the overall scores.

Table 10: Correlation coefficient between age and overall score

Correlation between age and overall score
-0.2

As the value is close to 0, this indicates a weak linear relationship between age and overall score; as age increases, the overall score slightly decreases.

Table 11: Regression analysis of age and overall score

Regression Analysis								
SUMMARY OUTPUT								
Regression Statistics								
Multiple R	0.19							
R Square	0.03							
Adjusted R Square	0.02							
Standard Error	9.57							
Observations	46							
ANOVA								
	df	*SS*	*MS*	*F*	*Significance F*			
Regression	1	167.23	167.23	1.82	0.18			
Residual	44	4029.64	91.58					
Total	45	4196.87						
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	79.46	19.08	4.16	0.00014	40.99	117.92	40.99	117.92
X Variable 1	-1.64	1.214	-1.35	0.18	-4.09	0.81	-4.09	0.81

The regression analysis further supports Table 8, suggesting that p value is more than 0.05, which indicates age is not a significant factor in the overall score.

Table 12: Regression analysis for age and awareness pre-simulation

SUMMARY OUTPUT								
Regression Statistics								
Multiple R	0.083							
R Square	0.007							
Adjusted R Square	-0.016							
Standard Error	1.184							
Observations	46							
ANOVA								
	df	*SS*	*MS*	*F*	*Significance F*			
Regression	1	0.432	0.4322	0.308	0.581			
Residual	44	61.676	1.408					
Total	45	62.109						
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	15.789	0.272	58.131	3.011	15.242	16.336	15.242	16.337
Do you know what phishing is?	-0.197	0.354	-0.555	0.581	-0.911	0.517	-0.911	0.518

From this analysis, we find that younger participants, on average, have some understanding of phishing knowledge; however, age is not a significant predictor for phishing knowledge.

Table 13: t-Test for confidence levels of distinguishing phishing emails between genders

t-Test: Two-Sample Assuming Unequal Variances		
	male	*female*
Mean	2.963	2.737
Variance	1.268	0.649
Observations	27	19
Hypothesized Mean Difference	0	
df	44	
t Stat	0.794	
P(T<=t) one-tail	0.216	
t Critical one-tail	1.68	
P(T<=t) two-tail	0.431	
t Critical two-tail	2.015	

The male mean confidence in identifying phishing is slightly higher than females; however, it would not be considered significant, and gender would not influence distinguishing phishing emails.

Table 14: t-Test comparing gender on how long they took to answer the email challenges

t-Test: Two-Sample Assuming Unequal Variances		
	male	*female*
Mean	55.65	46.45
Variance	1593.58	1864.53
Observations	162	114
Hypothesized Mean Difference	0	
df	231	
t Stat	1.80	
P(T<=t) one-tail	0.04	
t Critical one-tail	1.65	
P(T<=t) two-tail	0.07	
t Critical two-tail	1.97	

Males tend to take longer than females to answer the email challenges; however, both genders have taken a substantial amount of time to answer the simulation challenges.

Table 15: Correlation between age and duration of each challenge

	age	*Duration of each challenge*
age	1	
Duration of each challenge	0.11	1

There is a weak correlation between the age and duration of each challenge. Older participants tend to take longer on each challenge.

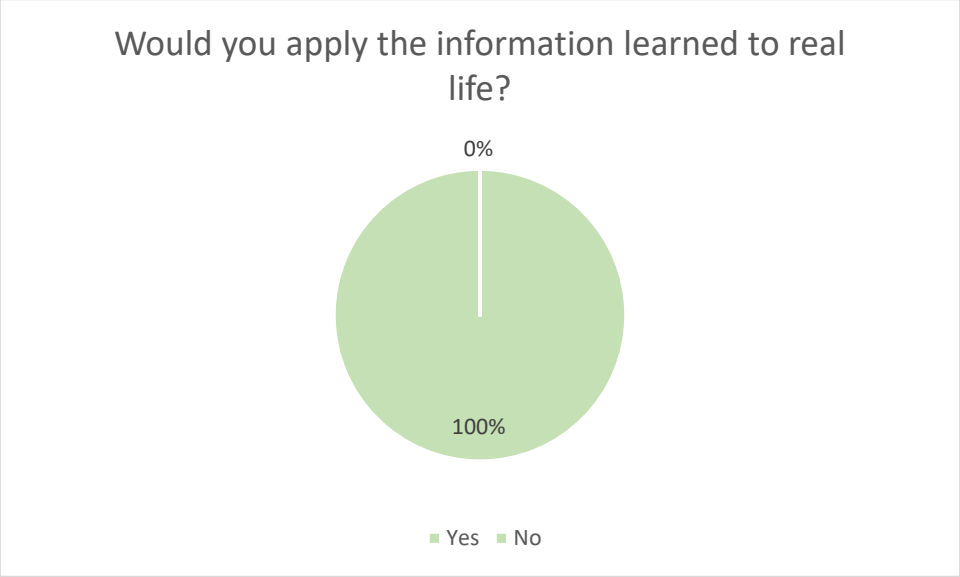


Figure 56: Participants indicating if they would apply learning from simulation in real life.

All participants felt they could apply the learning from the simulation in real-life scenarios.

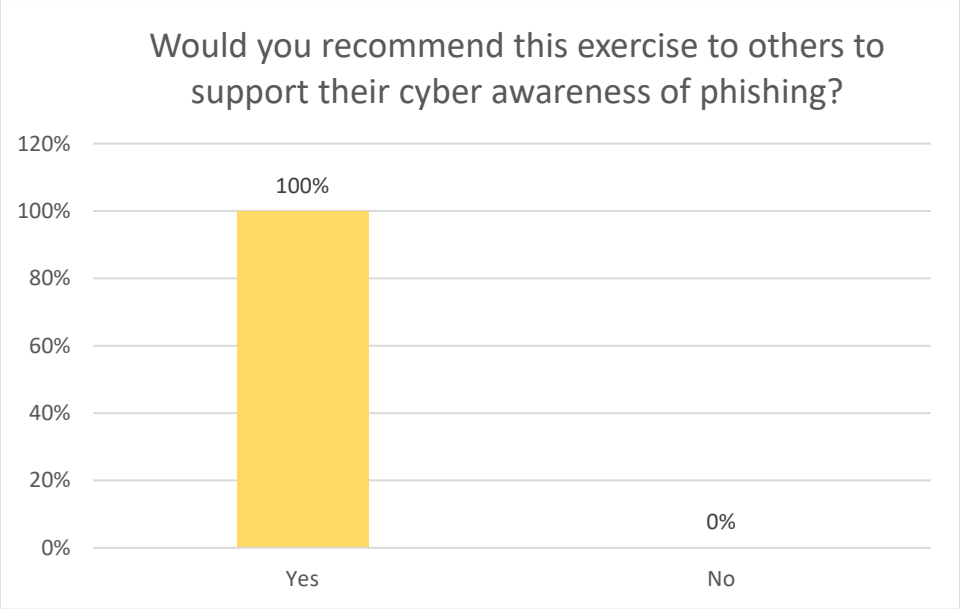


Figure 57: Participants recommendation of the simulation to others

All participants felt they would recommend the phishing simulation to others to support cyber awareness of phishing attempts.

Table 16: Regression to understand the relationship between accuracy and confidence

SUMMARY OUTPUT								
Regression Statistics								
Multiple R	0.26							
R Square	0.07							
Adjusted R Square	0.06							
Standard Error	0.70							
Observations	276							
ANOVA								
	df	*SS*	*MS*	*F*	*Significance F*			
Regression	1	9.67	9.67	19.45	1.48			
Residual	274	136.28	0.50					
Total	275	145.96						
	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	2.01	0.07	26.90	7.14	1.86	2.16	1.86	2.16
Accuracy	0.40	0.09	4.41	1.48	0.22	0.58	0.22	0.58

The analysis indicates a statistically significant positive correlation between decision confidence and accuracy in identifying phishing emails. More confident participants generally identified emails correctly; this does not imply causation, as high confidence does not guarantee accuracy, and other variables may be influential.

Table 17: Participants pre-simulation confidence against email challenge accuracy

	Pre-simulation confidence	*Email accuracy*
Pre-simulation confidence	1	
Email accuracy	0.11	1

The correlation between participants' confidence and their ability to identify phishing from genuine emails is positive but weak, with higher confidence correlating with marginally improved accuracy.

Table 18: Pre-simulation knowledge against accuracy in simulation performance

	Knowledge of phishing pre-simulation	*Accuracy scores*
Knowledge of phishing pre-simulation	1	
Accuracy scores	-0.14	1

The analysis suggests that participants who claimed to have more knowledge about phishing before the simulation tended to score lower in accurately identifying emails. However, the weak relationship and overconfidence may have played a part, which does not suggest causation.

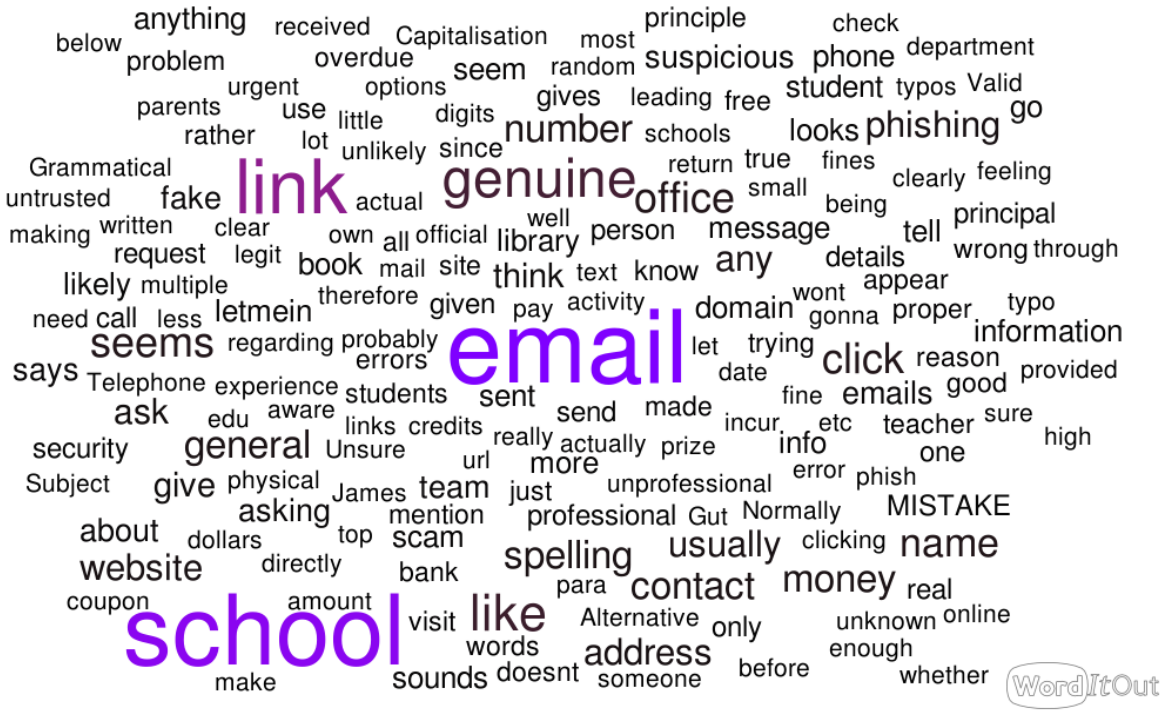


Figure 58: Word cloud on the most common terms used by participants in their reasoning response

The word cloud represents the most common terms used by participants. The terminology indicates that participants understand the nature of phishing content in email challenges and can provide decision-making responses.

Table 19: Comparision of NIST Phish Scale ratings and phishing simulation email challenges

Email Challenge	Cues	Level	Alignment	Score	Difficulty	Participant click rate	Participant accuracy
Challenge 1	12	Some cues	Medium	17	Moderately difficult	33%	76%
Challenge 2	8	Few cues	Medium	17	Very Difficult	11%	54%
Challenge 3	Not phishing email					9%	65%
Challenge 4	6	Few cues	High	30	Very Difficult	7%	67%
Challenge 5	12	Some cues	Medium	16	Moderately difficult	9%	46%
Challenge 6	Not phishing email					2%	98%

Email challenge 1, containing a relatively high number of cues and medium alignment, was moderately difficult, with 33% of participants clicking the link and 76% accurately identifying a phishing attempt.

Challenges 2 and 4, with 8 and 6 cues, were very difficult; they had a medium and high alignment, with participants scoring 54% and 67% in accuracy with lower click rates of 11% and 7%, respectively.

Challenge 5, which accumulated 12 cues and medium alignment, was rated moderately difficult, with 46% accuracy and a 9% click rate.

Genuine emails, Challenges 3 and 6, had varying accuracy of 65% and 98% and click rates of 9% and 2% respectively.

4.4 Discussion (2712 words)

Significant insights emerged from the simulation, notably:

i) Email challenge difficulty and performance.

Using the NIST Phish Scale (Dawkins & Jacobs, 2023), the complexity of email challenges was rated (Table 19), and a comparative analysis of participants' accuracy and click rates was conducted. The scale applies two dimensions: the first on observational cues such as spelling errors, tactics or visual indicators and the second on alignments such as replicating workplace processes, relevance, timing, promoting concern or not having warnings (Canham, 2022).

ii) Prior knowledge and performance.

Pre-simulation responses (Figure 12) highlighted participants' existing knowledge. The correlation between their perceived confidence and actual performance was analysed.

iii) Confidence and demographics.

The analysis between participants' demographics, such as gender and age, and their decision-making confidence was analysed to gauge self-efficacy in handling phishing threats.

4.4.1 Interpretation of the findings

i) Email Challenge 1 provided participants with numerous cues, leading to 33% clicking the URL link, but a majority of 76% correctly identified the phishing attempt. Participant observations commented, "Not personalised", "The email username is principal2897, I don't think an actual principal would use that name", and "abc_high_school in the email does not match with the website url, and they give out money unnecessarily". Some participants recognised the exaggeratedly optimistic content, commenting, "There's no way the school would give me free money", and "This is fake, because a thousand dollars is a ridiculous amount for a school to give to a student". Many did not over-elaborate in reasoning, providing instinctive reactions such as "seems unreal" and "gut feeling" (Figure 58). However, 24%

incorrectly identified this challenge showing that some participants could not register observational cues and were misled by seemly credible details such as “It is from a principal of the school and all the info is given including her phone no . and the reason for the mail”, “As its a genuine email from your own high school it dosent seem like they would phish you” and “States the Principal's name which wouldn't have been there if it was a phishing email”.

The trend in click rates, which reduced considerably (Figure 50), indicated a learning effect throughout the challenges; however, the challenge sequences were in a varied order and not uniform per participant. For Challenges 2, 3, 4 and 5, performance scores varied from 46% to 67%, suggesting these are challenging to identify. In contrast, Challenge 6 was accurately identified as genuine by nearly all participants, suggesting the content aligned more with their expectations of legitimate school communication. Participants commented, “I have seen this in the past”, “Collect the money in person. Genuine email”, “Email and domain appear real. Alternative contact info given, as well as instructions on how to claim that do not require you to click the link such as claiming at the office. Also value sum is small and realistic therefore not too good to be true”, and “In my experience, I have received emails from the school about the book coupon that looked like this”. Participants demonstrated heightened awareness with genuine emails, often referring to past experiences or logical processes such as collecting rewards in person. They can recognise realistic details like the smaller value of prizes and instructions that avoid clicking a link to indicate genuine emails.
The responses indicate that participants sensed familiarity in genuine emails and could identify cues similar to the school environment and aligning with the school rewards system.

The trend indicates that the higher the cues, the higher the success of participants identifying genuine or phishing emails. Participants seem to be cautious about numerous factors, such as the time it takes to make a decision, generally low click rates (Figure 50) and low click rates in genuine emails. There was a distinction between participants who could identify emails accurately and others who found this challenging, particularly in very difficult challenges (Table 19). The higher accuracy in Challenge 6 suggests that content elements in Challenge 3 must have been suspicious to participants as some commented, “I am not sure” and “They would call rather than sending an email”.

Challenges 2 and 4 were considered very difficult with lower accuracy despite low click rates, indicating participants were cautious about falling victim but unable to distinguish phishing

attempts. Participants commented identifying some cues and concerns, noting suspicious URLs or incorrect phone numbers "'www.letmein27834.com doesn't sound like a genuine website", "I did not request any email like this", "This is because the phone number has only 7 digits instead of 8." and inconsistencies with alignment "6000 is not a small money. It doesn't mention it is a school email", "unknown who I'm texting to" and "account is not a professional account like most people inquiring about financial grants".

However, there is clear evidence that some participants lack knowledge of cyber awareness by expressing uncertainty or misplaced trust in emails, commenting, "It doesn't seem suspicious", "I have no experience with these sort of emails", "looks as to be trustworthy since it doesn't ask for anything yet, not sure though", "As it is from the schools security team it should be safe" and "It's genuine because its from a school account". These findings underscore the necessity for more comprehensive cyber awareness training in practices as accuracy was mixed, especially with sophisticated attempts.

ii) Participants showed a moderate level of competency in identifying phishing, with an average score of 53.7 points, despite 78% reporting no formal cyber awareness training (Figure 39, Table 2). Interestingly, over half (58.7% Figure 43) knew what phishing indicates: informal learning sources such as peer discussions, media exposure or personal experiences. Therefore, whilst participants may not be formally trained, they are not entirely unaware that the quality of their knowledge sources is uncertain and, given the average score, suggests room for improvement.

A gender discrepancy emerged, with males generally perceiving themselves as more knowledgeable and confident in identifying phishing emails, a finding that merits further research and targeted educational policies to bridge the gap. Despite this perceived knowledge gap, females scored higher on average than males, challenging the notion of male dominance in cybersecurity awareness (Table 7).

Table 2: Descriptive analysis of participants' age and overall score in the phishing simulation

Participants professing prior knowledge (males 67%, females 33%) scored less than those who claimed they did not know (males 47%, females 53%, Table 8). Diaz et al. (2020) identified that higher self-efficacy can lead to higher susceptibility, which supports this finding that potential overconfidence in knowledge does not always translate to practical application. Age provided a weak inverse relationship with scores, suggesting younger participants have a greater awareness. This may be due to updated education curriculums or media exposure;

however, age was not a significant predictor of phishing knowledge in the regression analysis (Table 11, Table 12). These findings indicate the complexity of cyber awareness, highlighting informal learning influences and the need for educational strategies catering to different demographic groups.

iii) The confidence in decision-making identified some findings that support points already made. Most participants expressed confidence (Figure 46), with males displaying greater self-assuredness across all age groups (Figure 49). The confidence coincides with Table 16 as it significantly correlates with accurately identifying phishing attempts. Further analysis revealed that older participants took more time in decision-making; this did not necessarily correlate with lower confidence or ability. Interestingly, although males reported higher confidence, their deliberately extended decision-making time might indicate a more cautious or uncertain approach in practice. On average, both genders were confident of their ability to identify emails correctly, suggesting self-assurance was indicative of both genders. Whilst confidence is an asset to identify phishing attempts, the duration to respond with a decision could reflect a hesitant approach that a self-assessed confidence level may not capture.

4.4.2 Implications

i) The implications of the findings suggest the complexity of understanding participants' behaviours in the simulation and conducting a safe online lifestyle. Whilst low click rates will seem optimistic, the inconsistency in correctly identifying emails raises the concern that participants can misjudge genuine or phishing emails. The clear indicator would suggest greater cyber awareness training is needed, particularly on observing cues to support improved accuracy rates, particularly for challenging emails.

ii) The cyber awareness training gaps in knowledge perceived and derived from simulation scores identify that more training and education are required, mainly due to the deceptive nature of phishing attempts. Stakeholders in educational institutions may consider this a priority area to address. In addition, the inconsistency between actual and perceived knowledge indicated overconfidence in the simulation (Table 18). Participants considered that being overconfident could present more significant consequences for themselves by not adhering to adequate precautionary measures when handling suspicious emails. Whilst gender did not statistically

impact performance, there were significant differences in approach between genders, and this could be an area to explore more research into to reduce any gender gaps.

iii) As mentioned above, further training and education are required due to the varied performance and knowledge gaps. The room for improvement in accuracy and overall scores suggests that all participants would benefit from training. The positive response from participants that they felt they would recommend and consider simulations beneficial suggests that these could be an avenue to explore for schools. Confidence, whether over or underconfidence, indicates that training should be targeted and adapted to fulfil this need so confidence levels can better reflect participants' abilities.

4.4.3 Limitations

The critical limitation of the research is that the sample size of 47 participants was significantly smaller than expected. The findings and conclusions drawn from this research may not reflect the Hong Kong Secondary School's population and secondary students from Hong Kong in general. As seen in the data analysis (Table 7, Table 8, Table 9, Table 10), the relationships were statistically insignificant or weak to show any difference or effect in showing correlations or predictions. The results produced on regression analyses often did not produce significant results due to models not being given sufficient data. Due to the smaller sample, extreme values may also affect data, and minor effects that could provide exciting insights may go unnoticed. Furthermore, the comparative analysis opportunities were more challenging to complete to provide meaningful and reliable data. Ultimately, the sample size will affect the recommendations, suggesting they may not apply to broader studies in Hong Kong or globally but offer a starting point for research to continue in this area, particularly as previous work was limited.

The email simulation challenges could have provided more variety in terms of difficulty. Two challenges were genuine, two were moderately difficult, and two were very difficult, according to the NIST Phish Scale. Furthermore, the observational cues per challenge ranged from 6-12. Given the mixed-ability participants, the cues may need to be more explicit and in variable quantity. The content of the emails was based on the school environment; however, not all emails would require real-life links. One participant commented, "No reason to click a link."

that suggests a possibility that the click rate on certain emails may have been low and led to confusion in identifying between genuine and phishing emails.

The artefact could have included more security measures, such as multi-factor authentication for users, mainly if they regularly reviewed their simulation training. Rate-limiting implementation within a time frame could provide support in login.
The questionnaire forms provided valuable insights, particularly for quantitative data; however, more opportunities for qualitative data, such as responses to their choices, could have given even more depth of insight.

4.5 Recommendations and Evaluation

4.5.1 For Schools

The varied performance and knowledge gaps suggest schools incorporate regular cyber awareness phishing identification training/lessons as part of a dedicated curriculum incorporating cybersecurity, whether integrated across subject disciplines, in ICT or PSHE lessons. The constantly evolving nature of phishing attacks means that curriculums should be updated regularly so stakeholders are aware of the latest phishing tactics, can identify them, and can be confident and aware of mitigating them effectively.

The simulation gained a positive reception from participants who indicated they found the method beneficial. Conduct simulations regularly can promote knowledge and application whilst students get to test their knowledge against genuine and phishing emails. The opportunity to do this in a safe and controlled environment supports learning in a low-stakes setting.

Students in 21st Century learning require critical thinking skills to enhance the workforce and be leaders of tomorrow. Educators can promote critical thinking in phishing simulations so that they do not rely solely on observation cues but analyse the content and alignment of the email. Developing critical thinkers can take time, but it also can support other recommendations, such as addressing the issue of overconfidence and activities to support students in aligning their confidence levels with their actual skills to gauge self-assurance accurately. Allowing peer

learning opportunities for students to share their knowledge and strategies can reinforce and empower students. As the findings showed, many students produced high scores in the simulation, which may create student role models or leaders to encourage more students to pay attention to the concern of phishing. This could contribute to more students supporting future research project samples and closing any gender gaps.

As e-learning is vastly evolving and educators may feel less confident or trained to deliver lessons, collaboration with third parties could support it. Cybersecurity companies and national organisations may have school and community outreach programmes that deliver workshops, lectures and real-life insights from security professionals to support cyber awareness and gain further understanding of the threat landscape. Furthermore, expert support can mitigate any false information or misconceptions arising from students' personal experiences, peer sharing or media exposure and gain support for realistic confidence levels in knowledge or decision-making.

Raising cyber awareness and phishing is an issue facing society, and involving all stakeholders within education is critical. Parents/guardians may also be facing the same difficulties students are experiencing, and strategies that engage all stakeholders can reinforce best practices in school and at home and develop better digital citizens across society.

4.5.2 For future research

A larger sample size encompassing students from diverse backgrounds to show insights from various demographic groups. More statistically significant findings with predictive models and representative correlations would provide more robust conclusions. The improved quality of data gathered can offer increased areas of exploration, providing a strong foundation for future research. Further research extended from secondary school to primary school, university level or in professional industries could be included to provide comparative analysis, identifying trends throughout an educational life and building on the phishing studies already carried out extensively with the adult population—identification of uniqueness to specific demographic groups or Hong Kong to successfully mitigate phishing. Global studies could be conducted to recognise abilities to mitigate phishing attacks from different cultures or cultural backgrounds and identify trends as cyber threats can affect all societies.

The study was a one-off opportunity; however, extending the period of simulation assessment or periodic testing through a longitudinal approach could identify the long-term impact and retention of the phishing training when e-learning. The simulation can provide a progress log for students as they set up user accounts, supporting this concept. Furthermore, conducting a study over a longer time could allow training to occur in preparation for a simulation that may provide further valuable insights into retention rates and behaviours. Offering users the opportunity to change their password could be an additional application feature due to periodic use.

The simulation was conducted in a controlled environment with no consequences for any decisions made; however, it was developed so students could see how their performance may affect real life or identify the consequences of their actions. The URL links in the challenges could lead to a simulated consequence that may affect their overall score or provide a scenario for them to see where the consequence has led. Students would gain a deeper understanding and experience of phishing in closer to real-life settings whilst still being in a controlled and safe environment.

Further research is needed to explore other training methods that benefit students' cyber awareness, such as gamification, workshops or e-learning self-based courses, as some studies have already been conducted using these methods. Incorporating technology as a solution could be considered. Further research could examine the training of students when using solutions such as email filters or artificial intelligence to mitigate phishing attacks.

4.6 Conclusion (359 words)

Educational institutions play a crucial role in offering students the opportunity to enhance their knowledge and skills to manage their online lifestyles. Due to the increased risk and sophistication of phishing attacks, school leaders must design policies and educators support strategies to take proactive measures to ensure students are prepared with security best practices. Due to this study area still underdeveloped in research, there are more opportunities to gain deeper insights to enhance educational initiatives and gain valuable insights. The

artefact simulation has the potential to extend further to offer students more learning opportunities.

The simulation was a positive indicator to gauge students' phishing recognition abilities, and insights were drawn through meaningful data collected. There was an indication of student awareness of phishing whilst identifying areas to improve with the simulation, such as offering more qualitative data opportunities. The feedback from the post-simulation questionnaire indicated that students found this beneficial and would recommend it to others to be considered an effective tool for cybersecurity education. As there were a variety of performance scores and gaps in phishing recognition, the simulation successfully identified the strengths and limitations of the sample and areas for further development. Participants were engaged in the simulation, and the duration of completion was appropriate for secondary school students as it did not disrupt their regular routines. Whilst most of the data was meaningful, it is clear some responses were guesses rather than informed decisions due to their knowledge found in the qualitative data, and the small sample size could skew the data negatively and not provide a fair and reliable representation of the broader student population.

The project objectives were primarily met, and the hypothesis was proved true that students have cyber awareness and mitigate phishing attempts. The low rate of URL clicks and high accurate scoring suggests that students are cyber-aware to protect themselves online. Decisions to ignore URL links with high confidence testing hold the hypothesis to suggest that current educational efforts are effective in Hong Kong. Nevertheless, in areas where the hypothesis does not hold, further development is still necessary for knowledge gaps, and cybersecurity education enhancement is necessary.

5.0 Learning (674 words)

Reflecting on the learning, I have considered Rolfe et al. (2001) model based on the three simple questions: What? So What? and Now What? (Rolfe et al., 2001) to provide description, analysis and action points that could significantly contribute to improved practice.

What? – The experience

The experience involved engaging in a complex learning process that allowed me to advance my technical skills through Python programming software development. I encountered practical issues such as circular imports, designing routes, database migrations and adding user scoring features, which caused frustration but quality learning when problem-solving. Ethically, it broadened my mindset to understand the crucial role of privacy in research and maintaining integrity and professionalism with vulnerable participants. The preparation for ethical approval was challenging but enlightening.

In project management, the experience was rewarding by using previous experience to use Gantt charts for self-directed milestones and utilising the concept of co-configuration (Sun & Goodyear, 2020) to transform working methods of differing mindsets, such as effective organisation and agile development. Supervisory communication helped shape the outcomes by offering a scaffold of tasks that intrinsically motivated to keep on track extrinsically for project completion to produce meaningful research.

Ensuring a growth mindset allowed me to maintain a positive attitude even when faced with technical challenges or concept difficulties to surpass obstacles (Yeager & Dweck, 2020). Fixed mindsets may lead to avoiding challenges and conceal a lack of understanding (Campbell et al., 2020), which would have stalled progress, but dedication indicates that abilities are not fixed.

So What? – Analysis

Adaptability is crucial for success in problem-solving, project management and a growth mindset. Reflection is a process that was undertaken throughout the project stages to adapt technical knowledge and methodological approaches. The co-configuration method allowed

me to meet the project demands by aligning my learning style to transform challenges into opportunities for growth, which brought satisfaction. This flexibility of mind provided a basis for independent learning, which maintained professionalism throughout, such as managing sensitive data of vulnerable participants in the data collection stage. Even with obstacles such as sickness and timing, whereby students were absent or overwhelmed with paperwork to submit as it was during the first weeks of the academic year, the challenges helped build resilience into the project stage. When challenges are overcome, we can demonstrate reflexivity, responsiveness, adaptability and flexibility (Rahman et al., 2021).

Emotional responses varied throughout the process and were as important as the academic response, with periods of satisfaction when succeeding in data collection or producing the web application live compared to frustration and anxiety in the development stages of the artefact or identifying significant findings in the data analysis. Variations of stressors can be expected during the process, particularly combined with the distance learning methods of the course (Russell-Pinson & Harris, 2019). Resilience was built through these experiences, and encouraging supervisor feedback taught me the importance of perseverance to demonstrate self-determination theory (Ryan & Deci, 2020) to have an intrinsic desire to contribute to society with meaningful research on cyber awareness and phishing.

Now What? – Future application

The project has guided me to utilise transferable skills through lifelong learning to manage stress positively, be self-direct, and be time efficient to produce sound levels of learning and improve self-assurance. Utilising experience as a manager in the education sector, the traits and skills gained supported me in resilience and not accepting learned helplessness (Rizvi & Sikand, 2020) when facing misunderstandings in complex situations. Setting short-term goals and targets to pursue achievement motivation helps gain satisfaction from the work produced (Anderman, 2020).

For continuing professional development, I look forward to guiding young people to adhere to professional standards and codes of conduct to benefit society (British Computing Society, 2022), facilitating better digital citizenship. In addition, this would support the evolution of e-learning and technology integration.

The project has demonstrated growth in lifelong learning whilst setting new future priorities for my professional journey and setting a commitment to emotional resilience, adaptability, and ethical practice in my learning styles to produce further meaningful research for society.

6.0 List of References

Akacha, S. a.-L. & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability,* 15, (19): 14132.

Alhaddad, M., Mohd, M., Qamar, F. & Imam, M. (2023). Study of Student Personality Trait on Spear-Phishing Susceptibility Behavior. *International Journal of Advanced Computer Science and Applications,* 14, (5).

Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science,* 3.

Anderman, E. M. (2020). Achievement motivation theory: Balancing precision and utility. *Contemporary Educational Psychology,* 61, 101864.

Antunes, M., Silva, C. & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences,* 11, (23): 11269.

Association for Computing Machinery. (2023). ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 30 October 2023].

Bagui, S., Nandi, D., Bagui, S. & White, R. J. Classifying Phishing Email Using Machine Learning and Deep Learning. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 3-4 June 2019 2019. 1-2.

Barrientos, F., Jacobs, J. & Dawkins, S. 2021. Scaling the Phish: Advancing the NIST Phish Scale.

Birlea, M. C. (2020). Phishing Attacks: Detection And Prevention. *arXiv preprint arXiv:2004.01556*.

Boynton, M. H., Portnoy, D. B. & Johnson, B. T. (2013). Exploring the ethics and psychological impact of deception in psychological research. *IRB,* 35, (2): 7.

British Computing Society. (2022). Code of Conduct For BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 28 January 2023].

Broberg, R. & Sinnott, P. (2023). The Human Element of Cybersecurity: A Literature Review of Social Engineering Attacks and Countermeasures.

Cambridge Cem. (2023). About Cambridge CEM: We are Cambridge Centre for Evaluation & Monitoring. Available from: https://www.cem.org/about-us [Accessed 21 October 2023].

Campbell, A., Craig, T. & Collier-Reed, B. (2020). A framework for using learning theories to inform 'growth mindset' activities. *International Journal of Mathematical Education in Science and Technology,* 51, (1): 26-43.

Canham, D. M. (2022). Using NIST's Phish Scale to Optimize Employee Training. Available from: https://www.mimecast.com/blog/using-nists-phish-scale-to-optimize-employee-training/ [Accessed 20 October 2023].

Chau, C.-L., Tsui, Y. Y.-Y. & Cheng, C. (2019). Gamification for Internet Gaming Disorder Prevention: Evaluation of a Wise IT-Use (WIT) Program for Hong Kong Primary Students. *Frontiers in Psychology,* 10.

Cheung, A. (2023). Language Teaching during a Pandemic: A Case Study of Zoom Use by a Secondary ESL Teacher in Hong Kong. *RELC Journal,* 54, (1): 55-70.

Chowdhury, N. & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review,* 40, 100361.

Das, P. K., Mandal, A. P., Sinha, N. & Basava, A. (2020). *Data Privacy Preservation Based on Multitenant Isolation in Cloud*. EasyChair.

Dawkins, S. & Jacobs, J. How to Scale a Phish: An Investigation into the Use of the NIST Phish Scale. 2023. Proceedings of the Nineteenth Symposium on Usable Privacy and Security. [Accessed 19 September 2023].

Diaz, A., Sherman, A. T. & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia,* 44, (1): 53-67.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Personal Cyber Security Provision Scale development study. *Journal of Human Sciences,* 12, (2): 75-91.

Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H. & Derhab, A. An OWASP top ten driven survey on web application protection methods. Risks and Security of Internet and Systems: 15th International Conference, CRiSIS 2020, Paris, France, November 4–6, 2020, Revised Selected Papers 15, 2021. Springer, 235-252.

Garrison, D. R. (2016). *E-learning in the 21st century: A community of inquiry framework for research and practice*. Taylor & Francis.

Ghimire, D. (2020). Comparative study on Python web frameworks: Flask and Django.

Goel, S., Williams, K. & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems,* 18, (1): 2.

Gov.Uk, D. F. S., Innovation & Technology. (2023). Cyber security breaches survey 2023: education institutions annex. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex [Accessed 1 October 2023].

Greathorn. (2020). Phishing emails, explained: Attack Vectors targeting School Districts. Available from: https://www.greathorn.com/blog/phishing-emails-explained-attack-vectors-targeting-school-districts/ [Accessed 19 October 2023].

Ham, J. V. D. (2021). Toward a Better Understanding of "Cybersecurity". *Digital Threats,* 2, (3): Article 18.

Harris, C. J. (2016). The effective integration of technology into schools' curriculum. *Distance Learning,* 13, (2): 27-37.

Hartikainen, H., Iivari, N. & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction,* 22, 100146.

Henshaw, P. (2023). School cyber-attacks: Top three methods revealed. Available from: https://www.sec-ed.co.uk/news/school-cyber-attacks-top-three-methods-revealed-malware-ransomware-phishing-spoofing-education-hackers/#:~:text=The%20audit%20found%20that%20awareness,to%2035%25%20in%202019). [Accessed 26 March 2023].

Hindman, A. H., Wasik, B. A. & Bradley, D. E. (2019). How classroom conversations unfold: Exploring teacher–child exchanges during shared book reading. *Early Education and Development,* 30, (4): 478-495.

Hkcertcc. (2021). Annual Report. Available from: https://www.hkcert.org/f/press_center/909710/910908/HKCERT%20Annual%20Report%202021.pdf [Accessed 20 June 2023].

Ho, A., Ngai, A., Cheung, C., Shui-Ching, C., Yuen, A., Cheung, S. & Yeung, V. (2020). Enhancing Support for e-Learning in Schools. Available from: https://yrc.hkfyg.org.hk/en/2020/07/30/enhancing-support-for-e-learning-in-schools/ [Accessed 2 October 2023].

Ho, S. K. (2020). 91% of all cyber attacks begin with a phishing email to an unexpected victim. Available from: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html [Accessed 7 October 2023].

Hong Kong Education Bureau. (2020). Security Challenges & Prevention for Schools. Available from: https://www.edb.gov.hk/attachment/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/Information-Securtiy/20200113-Seminar/PPT-HKIRC-20200113.pdf [Accessed 7 October 2023].

Irwin, L. (2023). The worrying state of cyber security in schools. Available from: https://www.gdpr.co.uk/blog/the-worrying-state-of-cyber-security-in-schools [Accessed 7 October 2023].

Kyllonen, P. C. & Zu, J. (2016). Use of Response Time for Measuring Cognitive Ability. *Journal of Intelligence,* 4, (4): 14.

Lastdrager, E., Gallardo, I., Junger, M. & Hartel, P. (2017). *How Effective is Anti-Phishing Training for Children?*

Lee, Y. Y., Gan, C. L. & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health,* 20, (4): 3514.

Liu, J. (2022). Phishing attack 'highlights flaws in Chinese universities' cybersecurity'. Available from: https://www.timeshighereducation.com/news/phishing-attack-highlights-flaws-chinese-universities-cybersecurity [Accessed 7 October 2023].

Maharishi School. (2018). Phishing Emails – Taught by Shristi. Available from: https://maharishischool.org/school-news-blogs/phishing-emails/ [Accessed 19 October 2023].

Martin, A., Rashid Awais, Chivers, H., Danezis, G., Schneider, S. & Lupu, E. (2021). The Cyber Security Body of Knowledge v1.1.0. Available from: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf [Accessed 6 May 2023].

Mok, D. (2019). Hong Kong schools fall victim to cyberattack, raising fears for private data of pupils. Available from: https://www.scmp.com/news/hong-kong/law-and-crime/article/3041065/hong-kong-schools-fall-victim-cyberattack-raising [Accessed 7 October 2023].

Mycroft, C. (2023). Data of 900 Hongkongers exposed after hackers breach WhatsApp accounts of social services and schools. Available from: https://www.scmp.com/news/hong-kong/law-and-crime/article/3236906/hong-kong-whatsapp-hack-attack-compromises-accounts-900-people-after-fraudsters-target-instant [Accessed 7 October 2023].

Ng, T. K., Reynolds, R., Chan, M. Y. H., Li, X. & Chu, S. K. W. (2020). Business (teaching) as usual amid the COVID-19 pandemic: A case study of online teaching practice in Hong Kong. *Journal of Information Technology Education: Research*.

Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. & Anderson, P. (2020). *Investigating Teenagers' Ability to Detect Phishing Messages*.

Nicholson, J., Terry, J., Beckett, H. & Kumar, P. (2021). *Understanding Young People's Experiences of Cybersecurity*. *Proceedings of the 2021 European Symposium on Usable Security.* Karlsruhe, Germany: Association for Computing Machinery.

O'donnell, L. (2019). Back-to-School Scams Target Students with Library-Themed Emails. Available from: https://threatpost.com/back-to-school-scams-students-library-emails/148077/ [Accessed 19 October 2023].

Owasp. (2023). OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 22 October 2023].

Pcpd. (2023). Data Breach Notification. Available from: https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html [Accessed 22 June 2023].

Rahman, S. A., Tuckerman, L., Vorley, T. & Gherhes, C. (2021). Resilient Research in the Field: Insights and Lessons From Adapting Qualitative Research Projects During the COVID-19 Pandemic. *International Journal of Qualitative Methods,* 20, 16094069211016106.

Rayhan, A., Kinzler, R. & Rayhan, R. (N.D.). CYBERSECURITY BEST PRACTICES FOR PYTHON WEB APPLICATIONS.

Richardson, M. D., Lemoine, P. A., Stephens, W. E. & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning,* 27, (2): 23-39.

Rizvi, Y. S. & Sikand, R. (2020). Learned Helplessness at the Workplace and Its Impact on Work Involvement: An Empirical Analysis. *Global Business Review,* 0, (0): 0972150920976693.

Rodrigues, H., Almeida, F., Figueiredo, V. & Lopes, S. L. (2019). Tracking e-learning through published papers: A systematic review. *Computers & Education,* 136, 87-98.

Rolfe, G., Freshwater, D. & Jasper, M. (2001). *Critical reflection for nursing and the helping professions : a user's guide*. Houndmills, Basingstoke, Hampshire, Palgrave Houndmills, Basingstoke, Hampshire.

Ruiz, E. S. C., Vargas, R. P., Ortego, R. G., Meier, R., Saliah-Hassane, H. & Castro, M. (2023). *Vulnerability Assessment of Learning Management Systems*. IEEE Computer Society.

Russell-Pinson, L. & Harris, M. L. (2019). Anguish and anxiety, stress and strain: Attending to writers' stress in the dissertation process. *Journal of Second Language Writing,* 43, 63-71.

Ryan, R. M. & Deci, E. L. (2020). Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemporary Educational Psychology,* 61, 101860.

Sağlam, R. B., Miller, V. & Franqueira, V. N. L. (2023). A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education*, 1-13.

Sangrà, A., Vlachopoulos, D. & Cabrera, N. (2012). Building an Inclusive Definition of E-Learning: An Approach to the Conceptual Framework. *International Review of Research in Open and Distributed Learning,* 13, (2): 145-159.

Schmiedek, F., Oberauer, K., Wilhelm, O., Süß, H.-M. & Wittmann, W. W. (2007). Individual differences in components of reaction time distributions and their relations to working memory and intelligence. *Journal of experimental psychology: General,* 136, (3): 414.

Scmp. (2023a). Hong Kong sees drop in email phishing cases, but scam drill shows cybersecurity awareness 'still lacking'. Available from: https://www.scmp.com/yp/discover/news/hong-kong/article/3229674/hong-kong-sees-drop-

email-phishing-cases-scam-drill-shows-cybersecurity-awareness-still-lacking [Accessed 15 October 2023].

Scmp. (2023b). Hong Kong students made up fifth of online blackmail cases involving naked photos in first half of year, with youngest victim being 11 years old. Available from: https://www.scmp.com/yp/discover/news/hong-kong/article/3232510/hong-kong-students-made-fifth-online-blackmail-cases-involving-naked-photos-first-half-year-youngest [Accessed 15 October 2023].

Seth, P. & Damle, M. A Comprehensive Study of Classification of Phishing Attacks with its AI/I Detection. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), 18-19 Nov. 2022 2022. 370-375.

Shaikh, S., Khan, N., Sultana, A. & Akhter, N. Online Education and Increasing Cyber Security Concerns During Covid-19 Pandemic. International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022), 2023. Atlantis Press, 664-670.

Song, L. 2022. *Improving security of web applications based on mainstream technology.* Universitat Politècnica de València.

Sophos. (2023). The State of Ransomware
in Education 2023 Available from:
https://assets.sophos.com/X24WTUEQ/at/j74v496cfwh4qsvgqhs4pmw/sophos-state-of-ransomware-education-2023-wp.pdf [Accessed 15 October 2023].

Stanford University It. (2023). Recent Examples of Phishing. Available from: https://uit.stanford.edu/phishing [Accessed 19 October 2023].

Steed, M. (2023). How our school fought back after a cyberattack. Available from: https://www.tes.com/magazine/leadership/data/how-our-school-fought-back-after-cyberattack [Accessed 6 June 2023].

Sun, S. Y. H. & Goodyear, P. (2020). Social co-configuration in online language learning. *Australasian Journal of Educational Technology,* 36, (2): 13-26.

Turnbull, D., Chugh, R. & Luck, J. (2021). Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge? *Education and Information Technologies,* 26, (5): 6401-6419.

Unchit, P., Das, S., Kim, A. & Camp, L. J. Quantifying susceptibility to spear phishing in a high school environment using signal detection theory. Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings 14, 2020. Springer, 109-120.

Wang, C. & Xu, G. (2015). A mixture hierarchical model for response times and response accuracy. *British Journal of Mathematical and Statistical Psychology,* 68, (3): 456-477.

Yeager, D. S. & Dweck, C. S. (2020). What can be learned from growth mindset controversies? *American Psychologist,* 75, 1269-1284.

Zhang-Kennedy, L. & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.,* 54, (1): Article 12.

7.0 Bibliography

Belger, T. (2023). One in three schools hit by fraudsters impersonating staff emails. Available from: https://schoolsweek.co.uk/schools-hacked-cyber-incidents-advice-fraud-emails-results-day/#:~:text=Data%20leaks%20and%20email%20fraud,England%20at%2038%20per%20cent. [Accessed 27 March 2023].

Bolden, D. & Tymms, P. (2020). Standards in education: reforms, stagnation and the need to rethink. *Oxford Review of Education,* 46, (6): 717-733.

Census and Statistics Department. (2023). Table 720-90003 : Persons aged 10 and over who had used the Internet by sex and age group. Available from: https://www.censtatd.gov.hk/en/web_table.html?id=720-90003 [Accessed 20 October 2023].

Corsica. (2019). Phishing Email Example. Available from: https://www.corsicatech.com/wp-content/uploads/2019/04/Phishing-Email-Examples.pdf [Accessed 15 June 2023].

Digital Ocean. (2023). Product Documentation. Available from: https://docs.digitalocean.com/products/ [Accessed 29 August 2023].

Drüge, M., Fritsche, L., Bögemann, C., Apolinário-Hagen, J. & Salewski, C. (2022). Comparing stress, areas of stress and coping-strategies between distance-learning and on-campus students – A mixed-methods approach. *Frontiers in Psychology,* 13.

Glamoslija, K. (2023). What Is Phishing? Guide with Examples for 2023. Available from: https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-it/ [Accessed 28 June 2023].

Guido Van Rossum, Barry Warsaw & Coghlan., N. (2001). PEP 8 – Style Guide for Python Code. Available from: https://peps.python.org/pep-0008/#:~:text=The%20Python%20standard%20library%20is,inside%20parentheses%2C%20brackets%20and%20braces. [Accessed 26 June 2023].

Hkeaa. (2023). Table 2 : 2022 HKDSE Entry statistics. Available from: https://www.hkeaa.edu.hk/DocLibrary/HKDSE/Exam_Report/Examination_Statistics/dseexamstat22_2.pdf [Accessed 20 October 2023].

Hook Security. (2023). 10 Phishing Test Templates. Available from: https://f.hubspotusercontent30.net/hubfs/6535385/HookSecurity-10PhishingTestTemplates.pdf [Accessed 26 June 2023].

Irwin, L. (2023). Catches of the Month: Phishing Scams for May 2023. Available from: https://www.itgovernance.co.uk/blog/catches-of-the-month-phishing-scams-for-may-2023 [Accessed 11 June 2023].

Jay. (2022). Creating a Web App From Scratch Using Python Flask and MySQL. Available from: https://code.tutsplus.com/creating-a-web-app-from-scratch-using-python-flask-and-mysql--cms-22972t [Accessed 5 June 2023].

Kennedy, P. (2023). Testing Flask Applications with Pytest. Available from: https://testdriven.io/blog/flask-pytest/ [Accessed 19 August 2023].

Macmillan, N. A. 2001. Signal Detection Theory. *In:* SMELSER, N. J. & BALTES, P. B. (eds.) *International Encyclopedia of the Social & Behavioral Sciences.* Oxford: Pergamon.

Namecheap. (2023). SSL Certificates. Available from: https://www.namecheap.com/support/knowledgebase/category/14/ssl-certificates/ [Accessed 25 August 2023].

Pallets. (2010). SQLAlchemy Documentation. Available from: https://flask-sqlalchemy.palletsprojects.com/en/3.0.x/quickstart/ [Accessed 20 July 2023].

Pejić-Bach, M., Jajić, I. & Kamenjarska, T. (2023). A Bibliometric Analysis of Phishing in the Big Data Era: High Focus on Algorithms and Low Focus on People. *Procedia Computer Science,* 219, 91-98.

Python, R. (N.D.). Discover Flask. Available from: https://realpython.com/introduction-to-flask-part-2-creating-a-login-page/ [Accessed 10 June 2023].

Qualtrics. (2023). An introduction to t-test theory for surveys. Available from: https://www.qualtrics.com/uk/experience-management/research/t-test/#:~:text=What%20is%20a%20t%2Dtest,mean%20and%20a%20standard%20value. [Accessed 26 June 2023].

Robinson, B. (2023). Phishing difficulty explained. Available from: https://helpcentre.cybsafe.com/en/articles/8045374-phishing-difficulty-explained [Accessed 1 September 2023].

Shanee, D. & Jody, J. Federal Information Security Educators (FISSEA) Summer Virtual Forum 2023, Gaithersburg, MD, US. Phishing for User Context: Understanding the NIST Phish Scale. 2023-08-23 04:08:00 2023. Federal Information Security Educators (FISSEA) Summer Virtual Forum 2023, Gaithersburg, MD, US.

Sharma, K., Chiu, W.-Y. & Meng, W. (2023). *Security Analysis on Social Media Networks via STRIDE Model*.

Sqlalchemy. (2023). The Python SQL Toolkit and Object Relational Mapper. Available from: https://www.sqlalchemy.org/ [Accessed 18 June 2023].

Statista. (2023). E-learning and digital education - Statistics & Facts. Available from: https://www.statista.com/topics/3115/e-learning-and-digital-education/#topicOverview [Accessed 20 October 2023].

8.0 Appendices

Appendix 1: Signed external approval from the Hong Kong Secondary School to authorise student participation

[redacted]

Tel: [redacted] Fax: [redacted]

FAO Ethical Approval Panel
University of Essex
United Kingdom
Tuesday, 6 June 2023

Dear Sir/Madam

Researcher: Jonathan Joseph Callaghan

Regarding the above-named individual, we confirm that the research can take place for the Masters project at the [redacted] Hong Kong [redacted] on a sample of Secondary school students on the understanding that the right to privacy will be retained, i.e. the personal details of students will not be revealed.

Yours sincerely,

[redacted]

Principal

Appendix 2: Consent letter to participate

OPT IN REQUEST FORM TO PARTICIPATE IN RESEARCH

Examining the efficacy of Cybersecurity tools/techniques in implementing e-learning in Secondary schools in Hong Kong.

I hereby ***do*** consent for my child, _____ (Class : _____) (Class No:_____), to participate in the captioned project supervised by Dr Samuel Danso and Dr Cathryn Peoples of the University of Essex, United Kingdom, and the research conducted by Jonathan Callaghan, the staff member at YMCA of Hong Kong Christian College.

I understand and ***do*** consent that information obtained from this research may be used in future research and may be published. However, my right to privacy will be retained, i.e. the personal details of my child will not be revealed.

The procedure as set out in the **information sheet** has been fully explained. I understand the benefits and risks involved. My child's participation in the project is voluntary, as they can choose whether they want to participate.

I acknowledge that we have the right to question any part of the procedure and can withdraw at any time without negative consequences and still ***do*** consent to my child's participation.

	(Please tick for either yes or no)	YES	NO
1	I have read and understood the Participant Information Sheet for the above study and have been provided with a copy to keep.		
2	I have had the opportunity to ask the researcher questions about this research project.		
3	I understand I have the right to withdraw from the research at any time without giving a reason and that all information I have given will be destroyed.		
4	I understand that my identity will be protected by treating the information I provide anonymously, and it will be used solely by the researcher for the purpose of writing a report on the research project.		
5	I understand that the information I provide will be kept securely, and will not be revealed to any other party, and will be destroyed at the conclusion of the project.		
6	I understand that if I have any questions or concerns about how this research is being conducted, I can contact the independent person named in the Participant Information Sheet.		

I consent to participating in this research interview according to the information and principles described in the information sheet.

DECLARATION AND SIGNATURE/S

Signature: _____

Name of Parent / Guardian: _____

Date: _____

Appendix 3: Participant information sheet

Participant information sheet for parents/guardians

Research Project Title: Examining the efficacy of Cybersecurity tools/techniques in mitigating phishing when implementing e-learning in Secondary schools in Hong Kong.

Research Project Question: To what extent can cybersecurity tools/techniques empower secondary school students to mitigate social engineering attempts during e-learning?

Invitation

Your child has been invited to participate in this research project with the University of Essex as they have a unique insight into understanding cybersecurity awareness in secondary schools in Hong Kong.

Please decide if you wish your child to participate in this study. Before they take part, it is essential to ensure that you and they fully understand why the research is being undertaken and what is involved. Please take the time to read through the following information and ask any questions that you may have.

If you want more information or have concerns about this research project, please contact the researcher at jc21550@essex.ac.uk or see me in person.

Purpose of the research

The purpose of this research is primarily cyber security research. Since the Covid-19 pandemic, the adoption of e-learning by schools has accelerated faster than technology could be integrated and embedded into school curriculums. For students,

teachers and administrators, the implementation of e-learning was quickly absorbed into school environments with limited opportunities for training on cybersecurity awareness. A particular threat to the functionality of e-learning has been the social engineering attack of phishing which has also been one of the most common methods of attacks from malicious users in recent years.

Phishing is an attack used maliciously to deceive people into revealing sensitive information or installing malware on devices. Malware can disrupt or damage computers which criminals can exploit. Standard methods of phishing can come from emails or fraudulent websites.

Research suggests that many school curriculums inadequately educate students on phishing, leaving them vulnerable to cyber threats. The research project aims to assess your child's cybersecurity awareness concerning phishing attempts and empower them to make informed choices to manage their online lifestyle behaviours in the future. Participation in this research will also support schools to provide a better understanding of cybersecurity in their teaching and learning curriculums.

Where and when will this take place?

Your child's involvement in this research will be one session of approximately 10-20 minutes to complete. This will be completed after school in the Student Learning Centre which has glass doors and windows with additional staff members situated there to observe and help raise any concerns to the researcher. The room is useful as it is quiet and easily accessible.

As a participant, your child will complete a questionnaire assessing your cyber awareness knowledge and understanding. Then complete a phishing simulation exercise that will not be real or impact real life as it is solely for research purposes. During the simulation, your child will view a stimulus, such as a webpage or an email and decide whether they thought the stimulus was genuine. Following this, they will provide a reason/justification for that decision. Next, your child will select a score of confidence in making that decision, either low, medium, or high confidence. The responses will be timed. They then will answer further questions from the questionnaire to reflect on their cyber awareness after the simulation.

This study aims to prove that Secondary students in Hong Kong have cyber awareness to mitigate phishing attempts. From this, your child should be able to reflect on his/her current practice and online lifestyle behaviour whilst indirectly gaining education, training and awareness of phishing detection and mitigation. As the exercise is not a live event, no harm could occur, but hopefully, the awareness of this exercise provides you with information to make positive informed decisions on cybersecurity in the future.

What will your student have to do?

Data collection will use a mixed-method approach consisting of a quantitative and qualitative questionnaire. The project will also use action-based research by collecting data responses through a simulation programme. This means your child's results will contribute to the overall findings and are important.

Your child will be provided with a website to register a username and password. All personal details entered will be anonymised; this means no personal information will be able to be seen or shared as this will be secured in an encrypted database. The data collection will occur in September 2023 in school and will have time to complete it, which will not affect lessons or other learning.

Your child will then be provided with three tasks:

1) A questionnaire to self-assess cybersecurity awareness.
2) Presented with a phishing simulation to decide how they would respond to genuine or non-genuine examples. This will include an example of a webpage or email; they need to consider whether it was a phishing attempt.
3) A questionnaire to reflect on their responses.

Your child will then be required to log out and not be required for further participation. Once the research project is completed and published, the collected data will only be kept until December 2023.

The benefits of participation

The benefits of participating will support your child's learning and management of their online presence and behaviour. It may also provide a current assessment of their knowledge concerning the topic. Your child will also indirectly support research and good practice in schools. The identified gaps can support teachers and schools in their direction to meet cyber awareness learning objectives. Your child may find this process particularly useful to apply his/her knowledge in a practical manner rather than only theoretically in PSHE lessons.

The dangers of participation – Low risk

The concerns are that your child must understand the nature of a phishing simulation and that phishing attempts involve deception. This is not a live environment; all examples will not be real but designed to replicate what could happen when online. 'Not a live environment' suggests that the situation is not real and responses will not matter in real life. It is essential to understand this as the simulation information should not be shared or have opportunities to be misused in the future.

Data from the questionnaire will be anonymised so that each user has a unique identification number and other personal information remains private to the researcher. The collected data will not be shared or combined with other datasets, so there will be no opportunity to identify participants, and as mentioned, it will be stored in a secure database.

Technical security measures will be in place, such as secure coding practices, user authentication and authorisation, data encryption, use of HTTPS, secure database, input validation and sanitisation and administrative measures such as data minimisation, good privacy and third-party hosting security. If you would like to know more about these keywords, please ask.

Complaints and withdrawal from participation

The research is voluntary, and the participant can withdraw from the research at any time. All information related to the participant will remain confidential and only be identifiable by codes known only to the researcher.

If you wish to withdraw from the study, you can contact the researcher using the contact details provided, and all of the information and data collected from your personal identification number to date will be destroyed. Please email jc21550@essex.ac.uk to process the withdrawal from participation.

For whatever reason, you may wish to complain about the project. Should you wish to make a complaint, please address the complaint to the project Supervisor Dr Samuel Danso, at samuel.danso@kaplan.com.

There is no intention to cause emotional distress through your participation in this project; however, if it did happen, you and your child can seek support from the contact details below.

We have the Student Wellbeing Team on campus to support needs, including social workers and educational psychologists in the Wellbeing Office.

Jonathan Callaghan – jc21550@essex.ac.uk

Other links that may support you:

Cyber Security Information Portal https://www.cybersecurity.hk/en/learning-scam.php

CyberSec Hub https://cyberhub.hk/

Gov HK Technology Crime

https://www.gov.hk/en/residents/communication/infosec/cybersecurity/technologycrime.htm

Cyber Youth Programme

https://www.hkirc.hk/en/public_mission/cybersecurity/cyberyouth/

Who has ethically reviewed the project?

The research project will be ethically reviewed by the University of Essex Ethical Approval Panel and module tutors under the delegation from the Head of the Department. Furthermore, the school has also reviewed the process for permission to conduct the research.

Results of the research project

Once consent is given, the research results will be published in a project as part of the Master's degree programme at the University of Essex, United Kingdom, where there will also be a presentation to an academic panel. Please be aware that none of the participant's data and the school name will be mentioned to safeguard and protect the participants' identities. Only the group data will be disseminated to a broader audience,

and participants' individual responses will not be singled out. Participants will be referred to as 'Secondary students in Hong Kong'.

If participants would like to receive their individual results from the phishing simulation, a copy can be made available on request.

Further information

If you would like to obtain more information or have any concerns about this research project, please contact the researcher at jc21550@essex.ac.uk or telephone number 29883035.

Thank you for your interest in allowing your child to participate in this study.

Appendix 4: Pre-Simulation Questionnaire

1) What is your age?

2) What is your gender? (As per your national identity document)
   Male
   Female

3) Have you ever received any form of cyber awareness safety training or learning?
   Yes, I have been trained/had learning about it.
   No, I have never been trained/had any learning about it.

4) Do you know what phishing is?
   Yes, I do know what phishing is.
   No, I do not know what phishing is.

5) Have you ever received a message, email, or any other means that you suspected was a phishing attempt?
   Yes, I have received a suspected phishing attempt.
   No, I have not received a suspected phishing attempt.

6) How confidently could you distinguish between genuine and phishing emails on a scale of 1-5 (1=Low confidence, 5=Very strong confidence)?
   1 Low confidence
   2 Developing confidence
   3 Fairly confident
   4 Strong confidence
   5 Very strong confidence

7) How would you act if you received an email and suspected it to be malicious?
   Open the email to check the content
   Delete the email immediately
   Report the email

Unsure

8) Do you fully understand the potential consequences of being a victim of a phishing attempt, such as clicking on a URL website link from an unknown sender?
   Yes, fully understand.
   Partly understand.
   Do not fully understand.

Appendix 5: Post-Simulation Questionnaire

1) After completing the phishing simulation, has this increased your awareness and understanding of phishing?
   Yes
   No

2) How confidently do you think you could distinguish between genuine and phishing emails in the simulation on a scale of 1-5 (1=Low confidence, 5=Very strong confidence)?
   1 Low confidence
   2 Developing confidence
   3 Fairly confident
   4 Strong confidence
   5 Very strong confidence

3) From the phishing simulation, what did you find the most helpful?
   Identifying potential phishing emails
   Handling and managing emails
   Realising potential consequences
   It was not that helpful

4) How would you now act if you received an email and suspected it to be malicious?
   Open the email to check the content
   Delete the email immediately
   Report the email
   Unsure

5) After completing the simulation, will your online behaviour change? (Verifying sender details, cautious of URL clicking)
   Yes, I will be more attentive to what I click on or view.
   Perhaps, sometimes I will try to be more attentive and cautious.
   No, I will continue my normal behaviours; the simulation had no influence.

6) On a scale of 1-5, (1=Not effective at all, 5=Extremely effective), how effective was the simulation in educating you on phishing?

   1 Not effective at all

   2 Somewhat effective

   3 Moderately effective

   4 Very effective

   5 Extremely effective

7) Would you be able to apply the information learned from this exercise to real life?

   Yes

   No

8) Would you recommend this phishing exercise to others to support their cyber awareness of phishing?

   Yes.

   No.

Appendix 6: Participant debrief

1. What was the purpose of the research?

The purpose of this research is primarily educational research. Since the COVID-19 pandemic, the adoption of e-learning by schools has accelerated faster than technology could be integrated and embedded into school curriculums. For students, teachers and administrators, the implementation of e-learning was quickly absorbed into school environments with limited opportunities for training on cybersecurity awareness. A particular threat to the functionality of e-learning has been the social engineering attack of phishing, which has also been one of the most common methods of attacks from malicious users in recent years.

Research suggests that many school curriculums inadequately educate students on phishing, leaving them vulnerable to cyber threats. The research project aims to assess cyber awareness in this research and will also support schools in providing a better understanding of cybersecurity in their teaching and learning curriculums.

2. What did I complete, and what did the study aim to discover?

You completed a questionnaire assessing your cyber awareness knowledge and understanding as a participant. Then, you completed a phishing simulation exercise that was not real or had any impact in real life as it was solely for research. During the simulation, you viewed a stimulus, such as a webpage or an email and decided whether you thought the stimulus was genuine. You provided a reason/justification for that decision and a low, medium, or high confidence rating. Your response was also timed. You then answered further questions from the questionnaire to reflect on your cyber awareness. This study aims to prove that Secondary students in Hong Kong have cyber awareness to mitigate phishing attempts.

From this, you should be able to reflect on your current practice and online lifestyle behaviour whilst indirectly gaining education, training and awareness of phishing detection and mitigation. As the exercise is not a live event, no harm could occur, but hopefully, the awareness of this exercise provides you with information to make positive informed decisions on cybersecurity in the future.

3. How can I receive a summary of the results?

Should you wish to receive a copy of the results, please send the request to jc21550@essex.ac.uk, who will process the request. Please be aware that a summary will be provided. The result will be returned to the email address that requested the result. Please remember to provide your unique identification number in the email request.

4. What do I do if I wish to make a complaint?

For whatever reason, you may wish to complain about the project. Should you wish to make a complaint, please address the complaint to the project Supervisor, Dr Samuel Danso, at samuel.danso@kaplan.com.

5. Support agencies

Should anything from this process trigger any unpleasant or emotional worry, please remember that we have the Student Wellbeing Team on campus to support your needs, including social workers and educational psychologists.

Other links that may support you:

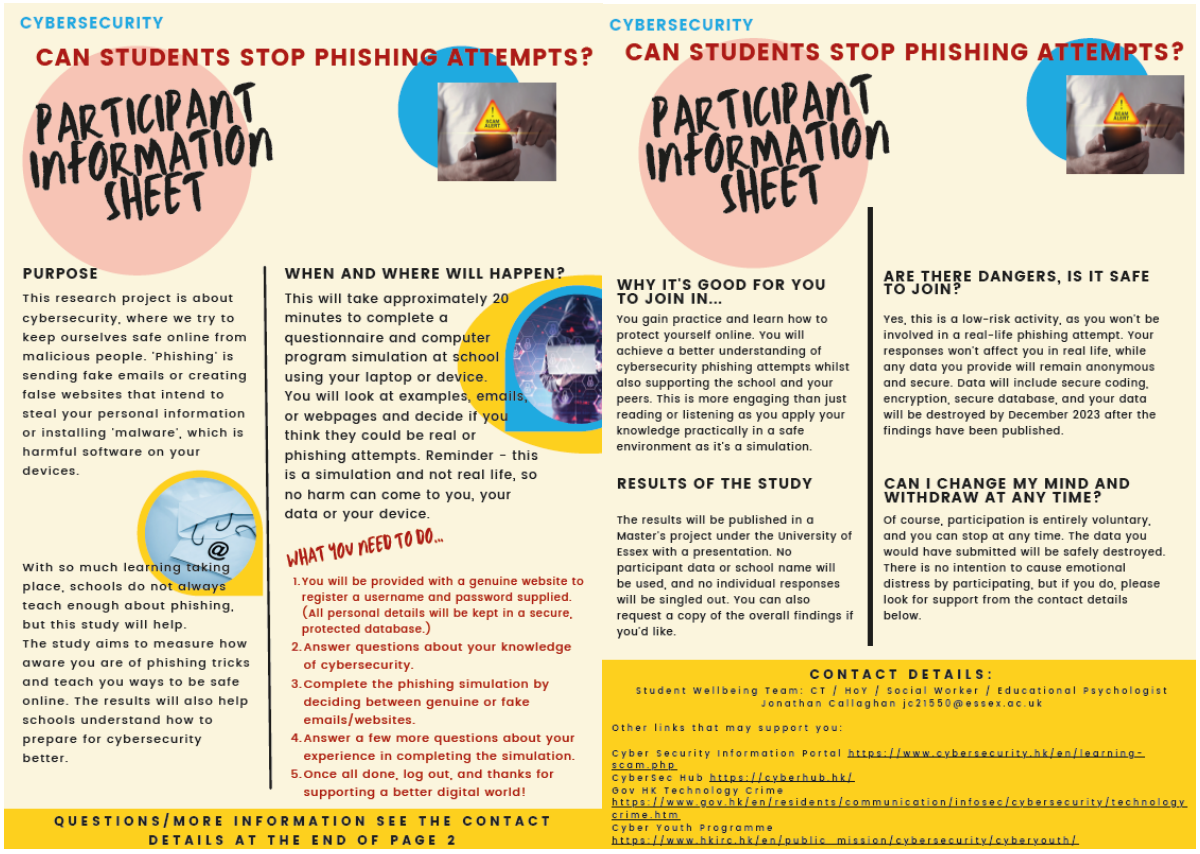
Cyber Security Information Portal https://www.cybersecurity.hk/en/learning-scam.php
CyberSec Hub https://cyberhub.hk/
Gov HK Technology Crime
https://www.gov.hk/en/residents/communication/infosec/cybersecurity/technologycrime.htm
Cyber Youth Programme https://www.hkirc.hk/en/public_mission/cybersecurity/cyberyouth/

6. Researcher contact details

If you would like to obtain more information or have any concerns about this research project, please contact the researcher at jc21550@essex.ac.uk.

Thank you again for taking part in this research.

Appendix 7: Student Snapshot Participant information sheet



CYBERSECURITY

CAN STUDENTS STOP PHISHING ATTEMPTS?

PARTICIPANT INFORMATION SHEET

PURPOSE

This research project is about cybersecurity, where we try to keep ourselves safe online from malicious people. 'Phishing' is sending fake emails or creating false websites that intend to steal your personal information or installing 'malware', which is harmful software on your devices.

With so much learning taking place, schools do not always teach enough about phishing, but this study will help.
The study aims to measure how aware you are of phishing tricks and teach you ways to be safe online. The results will also help schools understand how to prepare for cybersecurity better.

WHEN AND WHERE WILL HAPPEN?

This will take approximately 20 minutes to complete a questionnaire and computer program simulation at school using your laptop or device. You will look at examples, emails, or webpages and decide if you think they could be real or phishing attempts. Reminder - this is a simulation and not real life, so no harm can come to you, your data or your device.

WHAT YOU NEED TO DO...

1. You will be provided with a genuine website to register a username and password supplied. (All personal details will be kept in a secure, protected database.)
2. Answer questions about your knowledge of cybersecurity.
3. Complete the phishing simulation by deciding between genuine or fake emails/websites.
4. Answer a few more questions about your experience in completing the simulation.
5. Once all done, log out, and thanks for supporting a better digital world!

QUESTIONS/MORE INFORMATION SEE THE CONTACT DETAILS AT THE END OF PAGE 2

CYBERSECURITY

CAN STUDENTS STOP PHISHING ATTEMPTS?

PARTICIPANT INFORMATION SHEET

WHY IT'S GOOD FOR YOU TO JOIN IN...

You gain practice and learn how to protect yourself online. You will achieve a better understanding of cybersecurity phishing attempts whilst also supporting the school and your peers. This is more engaging than just reading or listening as you apply your knowledge practically in a safe environment as it's a simulation.

RESULTS OF THE STUDY

The results will be published in a Master's project under the University of Essex with a presentation. No participant data or school name will be used, and no individual responses will be singled out. You can also request a copy of the overall findings if you'd like.

ARE THERE DANGERS, IS IT SAFE TO JOIN?

Yes, this is a low-risk activity, as you won't be involved in a real-life phishing attempt. Your responses won't affect you in real life, while any data you provide will remain anonymous and secure. Data will include secure coding, encryption, secure database, and your data will be destroyed by December 2023 after the findings have been published.

CAN I CHANGE MY MIND AND WITHDRAW AT ANY TIME?

Of course, participation is entirely voluntary, and you can stop at any time. The data you would have submitted will be safely destroyed. There is no intention to cause emotional distress by participating, but if you do, please look for support from the contact details below.

CONTACT DETAILS:

Student Wellbeing Team: CT / HoY / Social Worker / Educational Psychologist
Jonathan Callaghan jc21550@essex.ac.uk

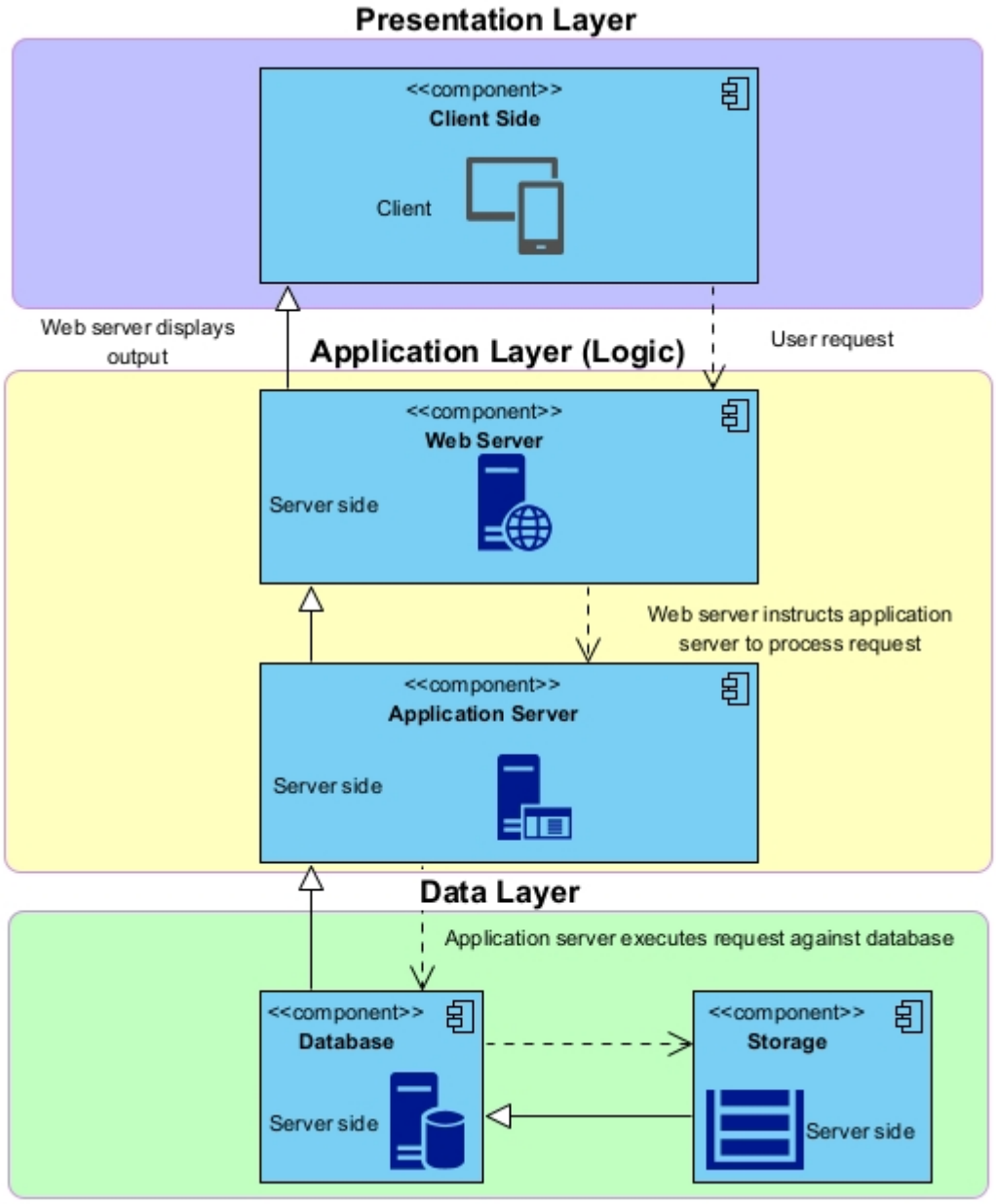
Other links that may support you:

Cyber Security Information Portal https://www.cybersecurity.hk/en/learning-scam.php
CyberSec Hub https://cyberhub.hk/
Gov HK Technology Crime https://www.gov.hk/en/residents/communication/infosec/cybersecurity/technologycrime.htm
Cyber Youth Programme https://www.hkirc.hk/en/public_mission/cybersecurity/cyberyouth/

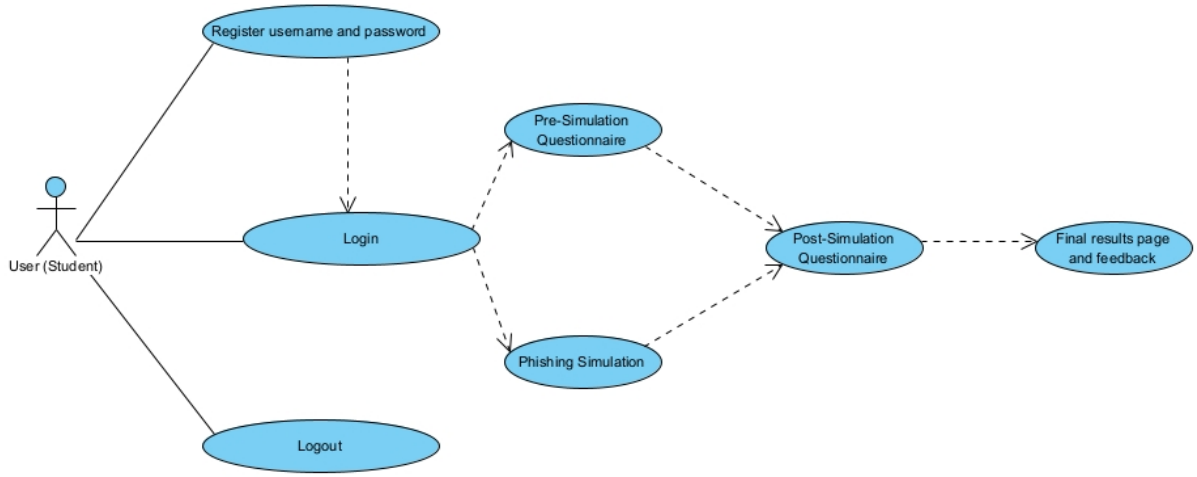
Appendix 8: Research project video advertisement for participants

https://drive.google.com/file/d/1p0lfzwJVJv3hKXVgGrUzOz9yAQjfVfNu/view?usp=sharing

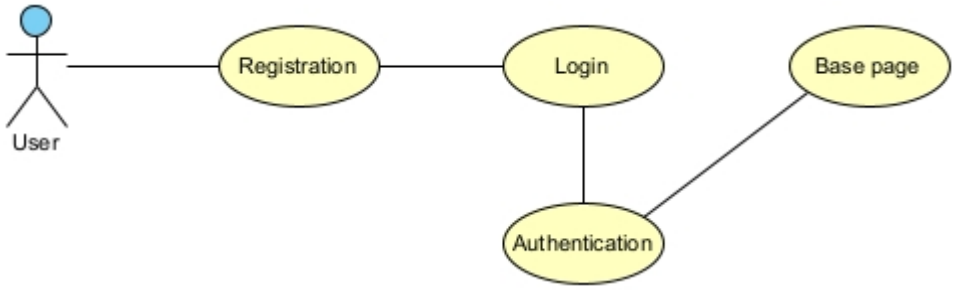
Appendix 9: Overview of three-tier architecture diagram



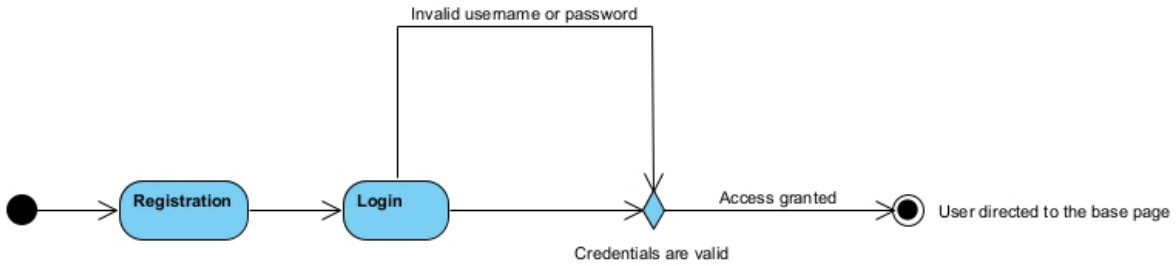
Appendix 10: Use case diagram for user common functions



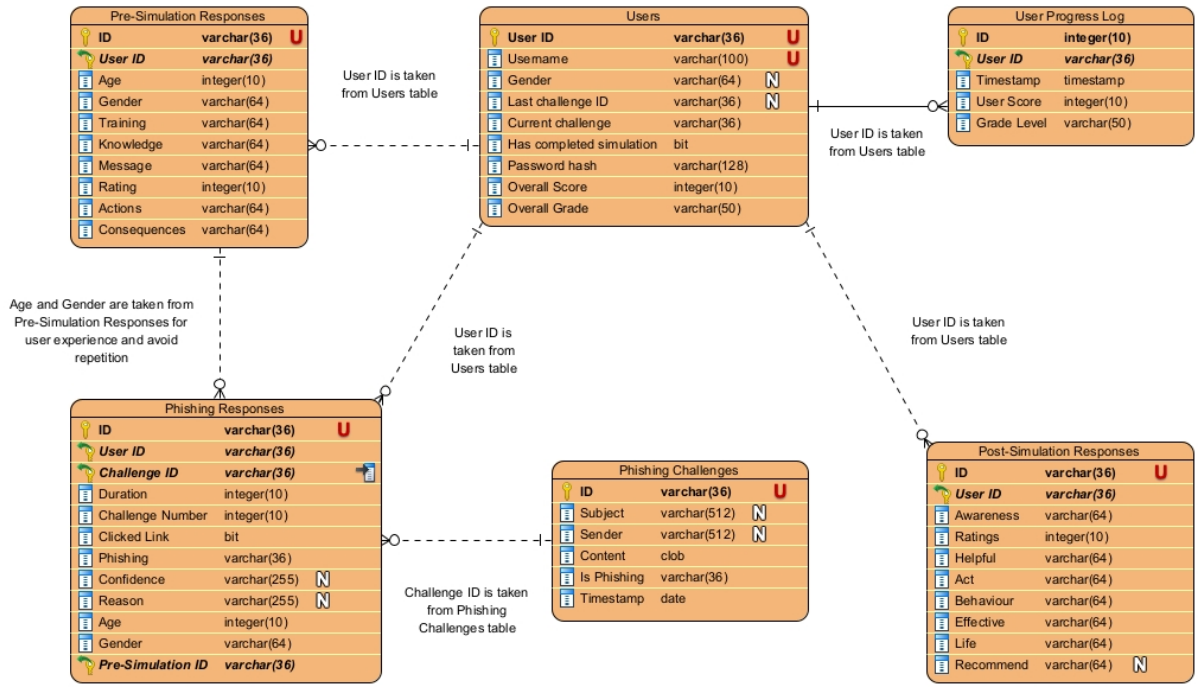
Appendix 11: Use case of user login



Appendix 12: Activity diagram of user login



Appendix 13: Entity-relationship diagram for database design



Appendix 14: Phishing simulation artefact repository

https://github.com/jj-call/Project-Phishing

Appendix 15: Summary of testing

Test type	Test case name	Description of test	Status
Functional	test_auth_views.py	Duplicate registration	Passed
		Invalid input	Passed
		Invalid login	Passed
		Login view	Passed
		Login whilst already logged in	Passed
		Logout	Passed
		Register route	Passed
		Valid login	Passed
		Valid registration	Passed
	test_extensions.py	Configuring database with login manager	Passed
		Configuring database	Passed
		Configuring migration	Passed
		Database exists	Passed
		Database models	Passed
	test_forms.py	Successful validation	Passed
		Validate without password	Passed
		Validate without username	Passed
		Invalid username	Passed
		Password mismatch	Passed
		Registration validated	Passed
		Pre-Simulation Questionnaire invalid age	Passed
		Pre-Simulation Questionnaire missing gender	Passed
		Pre-Simulation Questionnaire validation	Passed
	test_main_views.py	Index page	Passed
		Index uses the correct template	Passed
		Page not found	Passed
	test_models.py	New challenge	Passed
		New response	Passed
		New user	Passed
	test_simulation_views.py	User set password	Passed
		404 page	Passed
		Base route	Passed
		Base route requires login	Passed
		Get email	Passed
		Phishing simulation	Passed
		Phishing simulation invalid data	Passed
		Phishing simulation valid data	Skipped
		Pre-simulation questionnaire invalid data	Passed
		Pre-simulation questionnaire success	Passed
		Submit post-simulation	Passed
Unit	test_auth_views.py	Login view	Passed
		Register user	Passed
	test_extensions.py	Database instance	Passed
		Login manager instance	Passed
		Migrate instance	Passed

	test_forms.py	Invalid password mismatch	Passed
		Validation success 1	Passed
		Validation success 2	Passed
	test_init.py	Blueprints	Passed
		Configuration	Passed
		Configuration database	Passed
		Extensions	Passed
	test_models.py	Check password	Passed
		Example	Passed
		Password mismatch	Passed
		New user	Passed
		Set password	Passed
		Validate success	Passed
	test_simulation_views.py	Submit response	Passed

Appendix 16: Pytest functional tests

```
def test_duplicate_registration(self):
    # Register user
    _, _ = self.register_user()
    _, _ = self.register_user()
    with self.app.app_context():
        users = User.query.all()
        assert len(users) == 1
```

Tests/test_functional_test_auth_views.py::TestAuth::test_duplicate_registration PASSED [1%]

```
def test_invalid_input_register(self):
    response = self.test_client.get('/auth/register')
    soup = BeautifulSoup(response.data, 'html.parser')
    csrf_token = soup.find(id='csrf_token')['value']
    # Missing username
    self.test_client.post(
        "auth/register",
        data={"password": "test", "confirm_password": "test", "csrf_token": csrf_token}
    )
    with self.app.app_context():
        # This assert that no user was registered
        assert User.query.first() is None
```

Tests/test_functional_test_auth_views.py::TestAuth::test_invalid_input_register PASSED [3%]

```
def test_invalid_login(self):
    # Register a user
    self.register_user()

    # Attempt login with invalid password
    response_ = self.test_client.get('/auth/login')
    soup = BeautifulSoup(response_.data, 'html.parser')
    csrf_token = soup.find(id='csrf_token')['value']
    response = self.test_client.post(
        "auth/login", data={"username": "test", "password": "wrongpassword", "csrf_token": csrf_token}
    )
    assert b"/auth/login" in response.data
```

Tests/test_functional_test_auth_views.py::TestAuth::test_invalid_login PASSED [4%]

```
def test_login_view(self):
    response = self.test_client.get("auth/login")
    assert response.status_code == 200
    assert b"Login" in response.data
```

Tests/test_functional_test_auth_views.py::TestAuth::test_login_view PASSED [6%]

```
def test_login_while_already_logged_in(self):
    # Login once
    self.register_user()
    self.login_user()

    response = self.test_client.get("auth/login")
    assert response.status_code == 302  # Expect a redirect, as we are already logged in
```

Tests/test_functional_test_auth_views.py::TestAuth::test_login_while_already_logged_in PASSED [8%]

```
def test_logout(self):
    self.register_user()
    _, csrf_token_logout = self.login_user()

    # Perform logout
    response = self.test_client.post(
        'auth/logout',
        data={'csrf_token': csrf_token_logout}
    )
    assert response.status_code == 302
```

Tests/test_functional_test_auth_views.py::TestAuth::test_logout PASSED [9%]

```
def test_register_route(self):
    response = self.test_client.get("auth/register")
    assert response.status_code == 200
    assert b"Register" in response.data
```

Tests/test_functional_test_auth_views.py::TestAuth::test_register_route PASSED [11%]

```
def test_valid_login(self):
    # Register a user
    self.register_user()
    response, _ = self.login_user()
    assert response.status_code == 302
```

Tests/test_functional_test_auth_views.py::TestAuth::test_valid_login PASSED [13%]

```
def test_valid_registration(self):
    response, _ = self.register_user()
    with self.app.app_context():
        assert User.query.filter_by(username="test").first()
    assert response.status_code == 302
    assert response.location == "/auth/login"
```

Tests/test_functional_test_auth_views.py::TestAuth::test_valid_registration PASSED [14%]

```
def test_configuring_db(self):
    from my_app import login_manager
    if 'sqlalchemy' not in self.app.extensions:
        db.init_app(self.app)
    self.app.config['LOGIN_DISABLED'] = False
    assert isinstance(db, SQLAlchemy)
    assert self.app.config['LOGIN_DISABLED'] is False
```

Tests/test_functional_test_extensions.py::TestExtensions::test_configuring_db PASSED [16%]

```
def test_configuring_db_1(self):
    with self.app.app_context():
        assert db is not None
        assert isinstance(db, SQLAlchemy)

        assert db.engine is not None
```

Tests/test_functional_test_extensions.py::TestExtensions::test_configuring_db_1 PASSED [18%]

```
def test_configuring_migrate(self):
    migrate.init_app(self.app, db)
    assert migrate.directory == 'migrations'
```

Tests/test_functional_test_extensions.py::TestExtensions::test_configuring_migrate PASSED [19%]

```
def test_db_exists(self):
    with self.app.app_context():
        assert db is not None
        assert isinstance(db, SQLAlchemy)
```

Tests/test_functional_test_extensions.py::TestExtensions::test_db_exists PASSED [21%]

```
def test_db_models(self):
    from my_app.models import User
    assert User in db.Model.__subclasses__()
```

Tests/test_functional_test_extensions.py::TestExtensions::test_db_models PASSED [22%]

```
def test_login_manager_exists(self):
    with self.app.app_context():
        assert login_manager is not None
        assert isinstance(login_manager, LoginManager)
```

Tests/test_functional_test_extensions.py::TestExtensions::test_login_manager_exists PASSED [24%]

```
def test_migrate_exists(self):
    with self.app.app_context():
        assert migrate is not None
        assert isinstance(migrate, Migrate)
```

Tests/test_functional_test_extensions.py::TestExtensions::test_migrate_exists PASSED [26%]

```
def test_validate_success(self):
    with self.app.test_request_context():
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = LoginForm(csrf_token=csrf_token, username="username", password="password")
        assert form.validate() is True, "Form should be valid when all fields are provided"
```

Tests/test_functional_test_forms.py::TestForm::test_validate_success PASSED [27%]

```
def test_validate_without_password(self):
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = LoginForm(username='test', password='', csrf_token=csrf_token)
        assert form.validate() is False
        assert 'This field is required.' in form.errors['password']
```

Tests/test_functional_test_forms.py::TestForm::test_validate_without_password PASSED [29%]

```
def test_validate_without_username(self):
    with self.app.test_request_context():
        form = LoginForm(username='', password='test')
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form.csrf_token.data = csrf_token
        assert form.validate() is False
        assert 'username' in form.errors
```

Tests/test_functional_test_forms.py::TestForm::test_validate_without_username PASSED [31%]

```
def test_invalid_username(self):
    self.add_user(username='test')
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = RegistrationForm(username='test', password='test2', confirm_password='test2', csrf_token=csrf_token)
        assert form.validate() is False
        assert 'That username is taken' in form.username.errors[0]
```

Tests/test_functional_test_forms.py::TestRegistrationForm::test_invalid_username PASSED [32%]

```
def test_password_mismatch(self):
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = RegistrationForm(username='test2', password='test', confirm_password='test2', csrf_token=csrf_token)
        assert form.validate() is False
        assert 'Passwords must match.' in form.confirm_password.errors[0]
```

Tests/test_functional_test_forms.py::TestRegistrationForm::test_password_mismatch PASSED [34%]

```python
def test_validate_success(self):
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = RegistrationForm(username='test', password='test', confirm_password='test', csrf_token=csrf_token)
        assert form.validate() is True
```

Tests/test_functional_test_forms.py::TestRegistrationForm::test_validate_success PASSED [36%]

```python
def test_invalid_age(self):
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = PreSimulationResponseForm(age=100, csrf_token=csrf_token)
        assert form.validate() is False
```

Tests/test_functional_test_forms.py::TestPreSimulationForm::test_invalid_age PASSED [37%]

```python
def test_missing_gender(self):
    with self.app.test_request_context('/'):
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = PreSimulationResponseForm(age=20, csrf_token=csrf_token)
        assert form.validate() is False
```

Tests/test_functional_test_forms.py::TestPreSimulationForm::test_missing_gender PASSED [39%]

```python
def test_validate_success(self):
    with self.app.test_request_context():
        csrf_token = self.app.jinja_env.globals['csrf_token']()
        form = PreSimulationResponseForm(
            age=25,
            gender='male',
            training='yes',
            knowledge='yes',
            message='no',
            rating='3',
            actions='option1',
            consequences='option1', csrf_token=csrf_token)
        assert form.validate() is True
```

Tests/test_functional_test_forms.py::TestPreSimulationForm::test_validate_success PASSED [40%]

```python
def test_index(self):
    with self.app.app_context():
        response = self.test_client.get('/')
        assert response.status_code == 200
        assert b'<p>This application is intended for research data collection purposes.</p>' in response.data
```

Tests/test_functional_test_main_views.py::TestMainView::test_index PASSED [42%]

```python
def test_index_uses_correct_template(self):
    with self.app.app_context():
        response = self.test_client.get('/')
        # Test that the rendered template contains the content from the index.html template
        assert b'Home' in response.data
        assert b'Login' in response.data
```

Tests/test_functional_test_main_views.py::TestMainView::test_index_uses_correct_template PASSED [44%]

```python
def test_page_not_found(self):
    response = self.test_client.get('/invalid')
    assert response.status_code == 404
```

Tests/test_functional_test_main_views.py::TestMainView::test_page_not_found PASSED [45%]

```python
def test_new_challenge(self):
    with self.app.app_context():
        challenge = PhishingChallenge(
            subject='Test Subject',
            sender='test@example.com',
            content='This is a test challenge',
            is_phishing='genuine'
        )
        db.session.add(challenge)
        db.session.commit()

        assert challenge.subject == 'Test Subject'
```

Tests/test_functional_test_models.py::TestModels::test_new_challenge PASSED [47%]

```python
def test_new_response(self):
    with self.app.app_context():
        user = User(
            username='test',
            password='pwd123',
            gender='male'
        )

        db.session.add(user)
        db.session.commit()

        challenge = PhishingChallenge(
            subject='New Challenge',
            sender='test@example.com',
            content='Phishing content',
            is_phishing='phishing'
        )
        db.session.add(challenge)
        db.session.commit()

        response = PhishingResponse(
            user=user,
            challenge=challenge,
            duration=10,
            gender='male',
            challenge_number=1,
            clicked_link=True,
            phishing='phishing'
        )
        db.session.add(response)
        db.session.commit()

        assert response.user == user
```

Tests/test_functional_test_models.py::TestModels::test_new_response PASSED [49%]

```python
def test_new_user(self):
    with self.app.app_context():
        user = User(username='test', password='password123')
        db.session.add(user)
        db.session.commit()

        assert user.username == 'test'
        assert user.check_password('password123')
```

Tests/test_functional_test_models.py::TestModels::test_new_user PASSED [50%]

```python
def test_user_set_password(self):
    with self.app.app_context():
        user = User(username='test', password='initialpwd')
        db.session.add(user)
        db.session.commit()

        assert user.check_password('initialpwd')
```

Tests/test_functional_test_models.py::TestModels::test_user_set_password PASSED [52%]

```python
def test_404_page(self):
    with self.app.test_request_context():
        resp = self.test_client.get('/invalid')
        assert resp.status_code == 404
        assert b'Page Not Found' in resp.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_404_page PASSED [54%]

```python
def test_base_route(self):
    # Login the user
    self.register_user()
    resp, _ = self.login_user(follow=True)
    assert resp.status_code == 200
    assert b'Phishing Simulation' in resp.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_base_route PASSED [55%]

```python
def test_base_route_requires_login(self):
    with self.app.test_request_context():
        response = self.test_client.get(url_for('simulation.base'))
        assert response.status_code == 401
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_base_route_requires_login PASSED [57%]

```python
def test_get_email(self):
    with self.app.test_request_context():
        resp = self.test_client.get('/get_email')
        assert resp.status_code == 404
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_get_email PASSED [59%]

```python
def test_phishing_simulation(self):
    self.register_user()
    self.login_user()
    self.challenges()
    with self.app.test_request_context():
        response = self.test_client.get(url_for('simulation.phishing_simulation'))
        assert response.status_code == 200
        # Challenge content and form rendered
        assert b'alert(\'There was a problem submitting your response:' in response.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_phishing_simulation PASSED [60%]

```python
def test_phishing_simulation_invalid_data(self):
    # Invalid form data
    self.register_user()
    self.login_user()
    self.challenges()
    data = {
        'challenge_id': '123'  # invalid id
    }
    with self.app.test_request_context():
        response = self.test_client.post(url_for('simulation.phishing_simulation'), data=data)
        assert response.status_code == 400
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_phishing_simulation_invalid_data PASSED [62%]

```python
@pytest.mark.skip("passing data in test session is a challenge")
def test_phishing_simulation_valid_data(self):
    self.register_user()
    _, csrf_token = self.login_user()
    challenges = self.challenges()
    data = {
        'challenge_id': challenges[0],
        'response': 'phishing',
        'phishing': 'phishing',
        'confidence': 'high',
        'csrf_token': csrf_token
    }
    with self.app.test_client() as client:
        with client.session_transaction() as session:
            session['start_time'] = datetime.now().isoformat()
            with self.app.test_request_context():
                response = self.test_client.post(url_for('simulation.phishing_simulation'), data=data)
                assert response.status_code == 200
                assert b'Response saved successfully' in response.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_phishing_simulation_valid_data SKIPPED [63%]

```python
def test_pre_simulation_invalid_data(self):
    self.register_user()
    # Login and get CSRF token
    _, csrf_token = self.login_user()

    # Post invalid data with CSRF token
    data = {'age': 'foo', 'csrf_token': csrf_token}

    with self.app.test_request_context():
        response = self.test_client.post(url_for('simulation.submit_pre_simulation'), data=data)
        assert b'alert(\'Please select a gender.\')' in response.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_pre_simulation_invalid_data PASSED [65%]

```python
def test_pre_simulation_success(self):
    self.register_user()
    _, csrf_token = self.login_user()

    data = {
        'age': 25,
        'gender': 'male',
        'training': 'yes',
        'knowledge': 'yes',
        'message': 'no',
        'rating': '3',
        'actions': 'option1',
        'consequences': 'option1',
        'csrf_token': csrf_token
    }
    with self.app.test_request_context():
        response = self.test_client.post(url_for('simulation.submit_pre_simulation'), data=data)
        assert response.status_code == 302
        assert response.location == '/simulation/base'
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_pre_simulation_success PASSED [67%]

```python
def test_submit_post_simulation(self):
    self.register_user()
    _, csrf_token = self.login_user()

    with self.app.test_request_context():
        resp = self.test_client.post('/post_simulation',
                                     data={'age': 25,
                                           'gender': 'male',
                                           'awareness': 'yes',
                                           'ratings': '3',
                                           'helpful': 'option1',
                                           'act': 'option1',
                                           'behaviour': 'option1',
                                           'effective': '4',
                                           'life': 'yes',
                                           'recommend': 'yes',
                                           'csrf_token': csrf_token
                                           },
                                     follow_redirects=True)

        assert resp.status_code == 404
        # this appears to not found

    # Submit invalid form
    with self.app.test_request_context():
        resp = self.test_client.post('/post_simulation')
        assert b'<p>Sorry, the page you are looking for does not exist.</p>' in resp.data
```

Tests/test_functional_test_simulation_views.py::TestSimulation::test_submit_post_simulation PASSED [68%]

Appendix 17: Pytest unit tests

```
def test_login_view(self):
    with self.app.test_request_context():
        resp = self.test_client.get('/auth/login')
        assert resp.status_code == 200
```

Tests/test_unit_test_auth_views.py::TestUnitUser::test_login_view PASSED [70%]

```
def test_register_user(self):
    resp, _ = self.register_user()
    assert resp.status_code == 302
```

Tests/test_unit_test_auth_views.py::TestUnitUser::test_register_user PASSED [72%]

```
def test_db_instance(self):
    assert isinstance(db, SQLAlchemy)
```

Tests/test_unit_test_extensions.py::TestUnitUser::test_db_instance PASSED [73%]

```
def test_login_manager_instance(self):
    assert isinstance(login_manager, LoginManager)
```

Tests/test_unit_test_extensions.py::TestUnitUser::test_login_manager_instance PASSED [75%]

```
def test_migrate_instance(self):
    assert isinstance(migrate, Migrate)
```

Tests/test_unit_test_extensions.py::TestUnitUser::test_migrate_instance PASSED [77%]

```
def test_invalid_password_mismatch(self):
    with self.app.app_context(), self.app.test_request_context():
        form = RegistrationForm(data={
            'username': 'jc12345',
            'password': 'password123',
            'confirm_password': 'testpassword'
        })
        assert form.validate() is False
```

Tests/test_unit_test_forms.py::TestUnitForm::test_invalid_password_mismatch PASSED [78%]

```python
def test_validate_success_1(self):
    with self.app.app_context(), self.app.test_request_context():
        # Generate CSRF token
        csrf_token = generate_csrf()

        form = RegistrationForm(
            data={
                'username': 'jc12345',
                'password': 'password123',
                'confirm_password': 'password123',
                'csrf_token': csrf_token
            },
            meta={'csrf': True}  # Enable CSRF
        )
        # Validate the form and print errors
        form_valid = form.validate()

        # Actual assertion
        assert form_valid is True
```

Tests/test_unit_test_forms.py::TestUnitForm::test_validate_success_1 PASSED [80%]

```python
def test_validate_success_2(self):
    with self.app.app_context(), self.app.test_request_context():
        csrf_token = generate_csrf()
        form = RegistrationForm(data={
            'username': 'jc12345',
            'password': 'password123',
            'confirm_password': 'password123',
            'csrf_token': csrf_token
        })
        assert form.validate() is True
```

Tests/test_unit_test_forms.py::TestUnitForm::test_validate_success_2 PASSED [81%]

```python
def test_blueprints(self):
    assert 'auth' in self.app.blueprints
    assert 'simulation' in self.app.blueprints
```

Tests/test_unit_test_init.py::TestInit::test_blueprints PASSED [83%]

```python
def test_config(self):
    assert self.app.config['DEBUG'] is False
    assert self.app.config['TESTING'] is True
```

Tests/test_unit_test_init.py::TestInit::test_config PASSED [85%]

```python
def test_config_database(self):
    assert self.app.config['SQLALCHEMY_DATABASE_URI'] == my_app.config.TestingConfig.SQLALCHEMY_DATABASE_URI
    assert self.app.config['TESTING'] is True
```

Tests/test_unit_test_init.py::TestInit::test_config_database PASSED [86%]

```python
def test_extensions(self):
    assert 'sqlalchemy' in self.app.extensions
    assert 'migrate' in self.app.extensions
    assert 'login_manager' in dir(self.app)  # To assert that its been added to the app object
```

Tests/test_unit_test_init.py::TestInit::test_extensions PASSED [88%]

```python
def test_check_password(self):
    with self.app.app_context():
        user = User(username='jc12345', password='MyPassword')
        assert user.check_password('MyPassword') is True
        assert user.check_password('WrongPassword') is False
```

Tests/test_unit_test_models.py::TestUnitUser::test_check_password PASSED [90%]

```python
# Test example for the database
def test_example(self):
    # Create a new user instance
    with self.app.app_context():
        user = User(username="testusername", password="testpassword")
        # Add the user to the database
        db.session.add(user)
        # Commit the changes to the database
        db.session.commit()
        # Query the database and fetch the first row
        assert db.session.query(User).first() is not None
```

Tests/test_unit_test_models.py::TestUnitUser::test_example PASSED [91%]

```python
def test_invalid_password_mismatch(self):
    with self.app.app_context(), self.app.test_request_context():
            form = RegistrationForm(data={
                'username': 'jc12345',
                'password': 'password123',
                'confirm_password': 'testpassword'
            })
            assert form.validate() is False
```

Tests/test_unit_test_models.py::TestUnitUser::test_invalid_password_mismatch PASSED [93%]

```python
def test_new_user(self):
    with self.app.app_context():
        user = User(username='jc12345', password='some_password')
        assert user.username == 'jc12345'
        assert user.password_hash != 'testpassword123'
```

Tests/test_unit_test_models.py::TestUnitUser::test_new_user PASSED [95%]

```python
def test_set_password(self):
    with self.app.app_context():
        user = User(username='jc12345', password='some_password')
        assert user.check_password('some_password')
```

Tests/test_unit_test_models.py::TestUnitUser::test_set_password PASSED [96%]

```python
def test_validate_success(self):
    with self.app.app_context(), self.app.test_request_context():

            csrf_token = generate_csrf()

            unique_username = 'user' + uuid.uuid4().hex[0:16]

            form = RegistrationForm(data={
                'username': unique_username,
                'password': 'testpassword',
                'confirm_password': 'testpassword',
                'csrf_token': csrf_token
            }, meta={'csrf': True})

            assert form.validate()
```

Tests/test_unit_test_models.py::TestUnitUser::test_validate_success PASSED [98%]

```python
def test_submit_response(self):
    self.register_user()
    _, token = self.login_user()
    challenges = self.challenges()

    with self.app.app_context():
        # get user that has being registered
        user = User.query.first()
        # create challenger response
        pre_simulation = PreSimulationResponse(user_id=user.id, consequences='is_phishing',
                                               age=67, gender="Female", training='school 6',
                                               knowledge='math', message='testing', rating=7,
                                               actions='action maker')
        db.session.add(pre_simulation)
        db.session.commit()
        phis_response = PhishingResponse(user_id=user.id, challenge_id=challenges[0][0], duration=50,
                                         challenge_number=34, clicked_link=True, phishing=challenges[0][1],
                                         age=67, gender="Female", pre_simulation_id=pre_simulation.id)
        db.session.add(phis_response)
        db.session.commit()

    with self.app.test_request_context():
        # Send POST request
        response = self.test_client.post(f'/simulation/submit_response/{challenges[0][0]}',
                                         data={**{'perception': challenges[0][1]}, 'csrf_token': token})

        # Validate the response and the function call
        assert response.status_code == 200
```

Tests/test_unit_test_simulation_views.py::TestUnitSimulation::test_submit_response PASSED [100%]

Appendix 18: Pylint test for Auth_views.py

********** Module my_app.auth.views
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:61:0:
C0303: Trailing whitespace (trailing-whitespace)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:65:0:
C0305: Trailing newlines (trailing-newlines)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:1:0: C0114:
Missing module docstring (missing-module-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:13:0:
C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:30:0:
C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:35:0:
C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:38:4:
W1203: Use lazy % formatting in logging functions (logging-fstring-interpolation)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:57:15:
W0718: Catching too general exception Exception (broad-exception-caught)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:57:8:
W0612: Unused variable 'e' (unused-variable)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:10:0:
C0411: standard import "import logging" should be placed before "from flask import
render_template, request, flash, redirect, url_for" (wrong-import-order)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:2:0: W0611:
Unused Markup imported from markupsafe (unused-import)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:3:0: W0611:
Unused login_required imported from flask_login (unused-import)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\auth\views.py:5:0: W0611:
Unused generate_password_hash imported from werkzeug.security (unused-import)

Your code has been rated at 7.50/10 (previous run: 7.50/10, +0.00)

Appendix 19: Pylint test for simulation_views.py

********** Module my_app.simulation.views
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:520:0: C0301: Line too long (119/100) (line-too-long)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:525:0: C0301: Line too long (106/100) (line-too-long)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:1:0: C0114: Missing module docstring (missing-module-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:1:0: W0404: Reimport 'current_app' (imported line 1) (reimported)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:34:0: C0410: Multiple imports on one line (logging, random) (multiple-imports)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:44:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:44:24: W0621: Redefining name 'app' from outer scope (line 1) (redefined-outer-name)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:44:24: W0613: Unused argument 'app' (unused-argument)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:47:12: W0612: Unused variable 'i' (unused-variable)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:56:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:87:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:91:8: R1723: Unnecessary "elif" after "break", remove the leading "el" from "elif" (no-else-break)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:97:16: C0209: Formatting a regular string which could be an f-string (consider-using-f-string)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:109:0: C0116: Missing function or method docstring (missing-function-docstring)

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:121:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:171:15: W0718: Catching too general exception Exception (broad-exception-caught)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:189:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:189:0: R0914: Too many local variables (19/15) (too-many-locals)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:332:11: W0718: Catching too general exception Exception (broad-exception-caught)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:198:8: R1705: Unnecessary "elif" after "return", remove the leading "el" from "elif" (no-else-return)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:246:12: R1705: Unnecessary "else" after "return", remove the "else" and de-indent the code inside it (no-else-return)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:189:0: R0911: Too many return statements (7/6) (too-many-return-statements)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:189:0: R0915: Too many statements (55/50) (too-many-statements)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:252:16: W0612: Unused variable 'next_challenge' (unused-variable)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:339:0: C0116: Missing function or method docstring (missing-function-docstring)

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:345:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:356:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:372:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:374:4: R1705: Unnecessary "else" after "return", remove the "else" and de-indent the code inside it (no-else-return)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:419:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:443:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:458:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:463:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:515:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:532:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:556:0: C0116: Missing function or method docstring (missing-function-docstring)

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:562:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:568:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:574:0: C0116: Missing function or method docstring (missing-function-docstring)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:26:0: C0411: first party import "from my_app.forms import PhishingSimulationForm, PostSimulationForm, PreSimulationResponseForm" should be placed before "from ..extensions import db" (wrong-import-order)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:33:0: C0411: standard import "from datetime import datetime" should be placed before "from flask import Blueprint, request, render_template, flash, redirect, url_for, session, jsonify, current_app, current_app as app" (wrong-import-order)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:34:0: C0411: standard import "import logging, random" should be placed before "from flask import Blueprint, request, render_template, flash, redirect, url_for, session, jsonify, current_app, current_app as app" (wrong-import-order)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:34:0: C0411: standard import "import logging, random" should be placed before "from flask import Blueprint, request, render_template, flash, redirect, url_for, session, jsonify, current_app, current_app as app" (wrong-import-order)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\simulation\views.py:34:0: W0611: Unused import random (unused-import)

Your code has been rated at 8.17/10

Appendix 20: Flake 8 testing for forms.py

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:2:80: E501 line too long (167 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:3:80: E501 line too long (90 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:18:80: E501 line too long (90 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:20:80: E501 line too long (139 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:26:80: E501 line too long (91 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:28:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:30:80: E501 line too long (86 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:31:80: E501 line too long (112 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:32:80: E501 line too long (209 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:33:80: E501 line too long (171 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:34:80: E501 line too long (205 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:35:80: E501 line too long (217 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:36:80: E501 line too long (228 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:37:80: E501 line too long (196 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:40:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:43:80: E501 line too long (94 > 79 characters)

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:45:69: W291 trailing whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:46:80: E501 line too long (127 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:47:80: E501 line too long (102 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:50:43: W291 trailing whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:51:80: E501 line too long (113 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:52:80: E501 line too long (111 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:56:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:59:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:61:80: E501 line too long (106 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:62:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:65:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:66:1: W293 blank line contains whitespace
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:68:80: E501 line too long (109 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:69:80: E501 line too long (219 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:70:80: E501 line too long (267 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:71:80: E501 line too long (197 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:72:80: E501 line too long (325 > 79 characters)

c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:73:80: E501 line too long (224 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:74:80: E501 line too long (108 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:75:80: E501 line too long (118 > 79 characters)
c:\Users\jj_ca\OneDrive\Documents\GitHub\Project-Phishing\my_app\forms.py:77:1: W391 blank line at end of file