



MSc Computing Project Research Proposal and Ethical Approval Form

Student Details

| | |
|-----------------------------------|---|
| Student name | Jonathan Callaghan |
| Proposed title of research | Examining the efficacy of Cybersecurity tools/techniques in mitigating phishing when implementing e-learning in Secondary schools in Hong Kong. |
| Supervisor | Dr Samuel Danso and Dr Cathryn Peoples |

Section 1 Research Proposal

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

Introduction

The Covid pandemic in Hong Kong lasted from 20 January 2020 to 30 May 2023 (The Government of the Hong Kong Special Administrative Region, 2023). Hong Kong was unique in its strategy to manage the virus; however, this opened up opportunities for malicious attempts in the education sector. 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 via online platforms and video conferencing. Therefore 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. This came in the form of phishing attempts. Teaching staff could be emailed false website links or receive non-genuine emails posing as Principals or Senior Leaders. The acts had a denial of service (DoS) and ransomware demands (Steed, 2023).

Furthermore, during lessons, the inside threat was ever present, as many students were disgruntled at being faced with online learning and would attempt Zoom bombing attempts by sending out messages and requests to teachers to impose as genuine users to be allowed entrance to a Zoom meeting only to disrupt the lesson. The privacy and security settings required greater stringency so external malicious users did not 'zoom bomb' lessons and infiltrate school networks.

Phishing attacks increased significantly since 2020, with 48% of cases of cyber attacks in 2021, an increase of 7% (Hong Kong Computer Emergency Response Team Coordination Centre, 2021).

For schools in Hong Kong, the adoption of e-learning was accelerated, technological integration was not a seamless action, and the challenges of phishing attempts hindered school planning. As most planning strategies were a reactionary approach, few opportunities were considered for cybersecurity awareness and training for school stakeholders, whilst existing security protocols did not cater to new applications that teachers introduced to students for lessons. The inadequate preparation for students to manage their online behaviour and phishing made school stakeholders vulnerable to attacks.

The project aims to understand the cyber awareness of Secondary school students in Hong Kong regarding phishing. The project also aims to design a phishing simulation to evaluate the student's response capabilities and phishing awareness. The objective is to increase student efficacy in managing online behaviour, particularly detecting potential phishing attempts and managing sensitive data effectively.

The indirect benefits of the project include supporting schools to provide a better understanding of students' level of cybersecurity awareness when dealing with phishing attempts and allowing school leaders to incorporate cybersecurity knowledge, understanding and techniques into the teaching and

learning curriculums. As schools regularly review lesson plans and schemes of learning for evaluation, the finds of the study could positively influence intervention strategies to improve the teaching curriculums across subject disciplines as technology is integrated into all subject departments.

Skeleton of Literature Review

1. INTRODUCTION

a) Background

The adoption of e-learning in schools has led to rising cases of students being easily targeted by threat actors, and phishing attacks have seen a significant rise.

Whilst many schools provide learning in school curriculums, there are gaps in students' knowledge of how to protect themselves and the techniques support members can offer to minimise impact. There is also limited scope in how students can mitigate phishing attempts or be cyber-aware of threats. Threats can have physical, emotional and social repercussions.

The audience is aimed to be secondary school students, parents, academic teaching staff and cyber security researchers.

The secondary sources were selected through online library databases and search engine results. Searches were narrowed using search tools such as "_" for key terminology + and – to add or remove unwanted search results.



b) Scope

- A. Challenges to integrating technology in schools' curriculums.
- B. The increase in e-learning adoption by schools.
- C. Cyber awareness of students and practices.
- D. Phishing attempts on schools.
- E. Implementation of techniques to mitigate phishing attempts.

Will not be covered:

- Other cyber-attack methods on students or schools

2. BODY

A. Challenges of integrating technology in school curriculums

i) Environment to integrate technology into curriculums (Harris, 2016)

| | |
|--|--|
| <u>Research method:</u> | Qualitative |
| <u>Main findings:</u> | <p>Teachers need involvement with administrators.</p> <p>Teachers need an environment to be decision-makers on methods of integration for motivation.</p> <p>Committees gain peer support.</p> <p>Technology training is imperative.</p> |
| <u>Strengths</u> | <u>Limitations</u> |
| Identifies the environment needed, which is the opposite of Hong Kong during the pandemic years. | <p>Some views are dated.</p> <p>Conclusions suggest more research is needed for best practices of technology integration.</p> |
| <u>Discrepancies:</u> | Technology has made blended learning possible in Hong Kong through online classes but a barrier to effective teaching and learning. Learners need to socialise |

| | |
|--|---|
| | with each other, digital divide with staff, data privacy concerns and professional leadership challenges. (Ng et al., 2020) |
|--|---|

ii) Technology integration in school curriculums has made it challenging to define e-learning conclusively (Sangrà et al., 2012)

| | |
|--|--|
| <u>Research method:</u> | Mixed |
| <u>Main findings:</u> | <p>E-learning refers to learning that occurs when resources are used beyond technology.</p> <p>E-learning is a new dynamic for the 21st Century learning.</p> |
| <u>Strengths</u> | <u>Limitations</u> |
| E-learning is a new way of learning or improvement on existing education and technology-driven | <p>Dated as definitions of e-learning as evolved with technological advancement</p> <p>The experts involved were mainly higher education staff.</p> |
| <u>Discrepancies:</u> | E-learning should encompass electronic, mobile, and digital learning to enhance students' learning experience (Rodrigues et al., 2019) (Basak et al., 2018) |

B. The increase in e-learning adoption by schools

i) Institutions' response to adopted e-learning (Turnbull et al., 2021)

| | |
|--|--|
| <u>Research method:</u> | A mixed and integrative review |
| <u>Main findings:</u> | <p>Identification of standard technologies used in learning.</p> <p>Blended learning style.</p> <p>Online competence was an issue.</p> <p>Ad hoc approach to privacy and confidentiality.</p> <p>Identified lack of digital literacy in departments.</p> <p>Academic dishonesty.</p> <p>The COVID-19 pandemic has accelerated the adoption of e-learning in secondary schools (Clark, 2021, Duffin, 2022).</p> |
| <u>Strengths</u> | <u>Limitations</u> |
| <p>Comprehensive e-learning transition.</p> <p>Information from a range of countries, including China.</p> | <p>Focus on Higher Education specifically.</p> <p>Literature is focused on English-only publications during the pandemic.</p> |

C. Cyberawareness of students and practices

i) Students' knowledge of online protection (Zorlu, 2022)

| | |
|-----------------------------|--|
| <u>Research method:</u> | Quantitative |
| <u>Main findings:</u> | Users of the internet are more likely to be cyber aware. Educational lessons on security would benefit. |
| <u>Strengths</u> | <u>Limitations</u> |
| Awareness scales to measure | 401 participants (75.1% female) |
| <u>Discrepancies:</u> | No relationship between cyberbullying awareness and cyberbullying others. |

ii) Students trends and cybersecurity practices (Nicholson et al., 2021)

| | |
|--|--|
| <u>Research method:</u> | Quantitative |
| <u>Main findings:</u> | Students have a good knowledge of cybersecurity risks, practices and tools. While implementing initially, they disregard it over time due to usability. |
| <u>Strengths</u> | <u>Limitations</u> |
| The methodology supported a positive response from participants. | The research was performed in a live environment, and more safe environment was needed. |

| | |
|------------------------------------|--|
| They identified curriculum issues. | |
| Staffing expertise and efficacy. | |
| <u>Discrepancies:</u> | WIT program has benefits in supporting students to positive online behaviour and cyber awareness (Chau et al., 2019) |

D. Phishing attempts on schools

- i) Phishing is a prevalent form of social engineering that disrupts e-learning (Lastdrager, 2014) (Diaz et al., 2020).

| | |
|---|---|
| <u>Research method:</u> | Mixed |
| <u>Main findings:</u> | Students who understood phishing attacks performed worse in the experiment. Therefore they could be considered to overestimate their knowledge. |
| <u>Strengths</u> | <u>Limitations</u> |
| Identifies an underdeveloped area of research and requirement for students to learn about phishing, with nearly 70% of subjects clicking the phishing link. | It is aimed at university-level students. Not all participants realised it was an experiment. |
| <u>Discrepancies:</u> | Existing strategies for phishing awareness often overlook simulations, which could be valuable for secondary school students (Irwin, 2023) (Sağlam et al., 2023). |

| | |
|--|---|
| | Threats can arise internally and externally, including spoofing and impersonating school emails (Lastdrager et al., 2017) (Distler et al., 2021) (Sharma et al., 2023). |
|--|---|

E. Implementation of techniques to mitigate phishing attempts

- i) Importance of self-efficacy in protection (Lee et al., 2023)

| | |
|--|---|
| <u>Research method:</u> | Mixed |
| <u>Main findings:</u> | <p>Gaining anti-phishing knowledge can increase victimisation as users perceive overconfidence; however, the focus is on instant messaging phishing only.</p> <p>Phishing awareness, education, and training should be continued to raise self-efficacy and competence.</p> |
| <u>Strengths</u> | <u>Limitations</u> |
| Debate on users who share personal information online. The study suggests that those who protect their information are less likely to be phishing victims. | <p>The study is not confined to Hong Kong and has a broad age range of participants (up to 43 years).</p> <p>Cyberawareness focused on age and gender, and more demographics could be considered.</p> |

| | |
|------------------------------|---|
| <p><u>Discrepancies:</u></p> | <p>Current school curriculums inadequately educate students on phishing, leaving them vulnerable to cyber threats (Henshaw, 2023) (Nicholson et al., 2020) (Belger, 2023).</p> <p>Businesses also face phishing attacks, emphasising the need for educational training.</p> |
|------------------------------|---|

3. CONCLUSION

E. Identify the research that is most significant to the research question.

F. Indicate the significant research gaps in the literature.

G. Justification for this literature review to support the research gaps.

H. Recommended outcomes from the review.



Research methods

The project will undertake empirical research to identify the current approaches to phishing from the literature review and design the simulation accordingly to the findings. Data collection would occur from the simulation to record the actions and behaviours (Wheelan, 2013). The simulation will offer conclusive platforms to collect data in a safe and controlled environment. The simulation will not be real, so participants involved will not need to worry about any responses they make that could affect them daily.

The participants are under the age of 18 years, which adds complexity to the data collected, such as anonymity, privacy and safeguarding vulnerable people. The simulation will be conducted in a safe school environment in the researcher's presence as a qualified and registered educator, surrounded by supportive staff to ease the well-being concerns of participants. The application will collect data from participants' inputs, deciding whether the stimuli presented, such as an email or webpage, is genuine or non-genuine. The response will be timed to make the decision, and the participants will justify the decision and a rating score of how confident they are in their decision. This is also considered action research, with participants' input directly influencing the results.

Independent variable: Phishing attempt on the Secondary students.

Dependent variable: Decision made through the level of cyber awareness and ability to mitigate.

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

The project will aim to correlate the data with the demographic group (Secondary school students in Hong Kong) by assessing their cyber awareness knowledge through multiple choice and open questions in surveys undertaken before and after the simulation. The mixed method approach will gather quantitative

and qualitative data (Dawson, 2009) to record participants' perceived awareness and ability to mitigate phishing attempts.

Primary evidence will be collected from the surveys and simulation, while secondary evidence will be researched from literature reviews and statistical reports that can support the data analysis.

The questionnaire's design will aim to measure participants' knowledge and awareness of phishing, and the similarities in pre and post-simulation questionnaires are intended to facilitate greater accuracy in comparison.

The simulation design will provide quantitative data for analysis so that variables can be categorised easily and tabulated. Statistical analysis of mean, median, mode and standard deviation can be derived from the data collected to show the distribution of results and allow visual graphical interpretation and qualitative interpretation of participants' performance.

Furthermore, statistical tests such as T-tests (Qualtrics, 2023) to prove or disprove a null hypothesis with a paired t-test can support in determining any statistical difference in the means of the pre and post-simulation questionnaires. Greater interpretation of the results of these tests with comparison to the p-value and chosen significance level will allow more understanding of the effect of the simulation on students' knowledge and awareness of phishing attacks.

Description of artefact

The artefact will be a web-based application with a questionnaire and phishing simulation to assess participants' cyber awareness and collect responses.

The artefact will be produced in the Python Flask framework. Participants can log into the application to complete pre and post-simulation questionnaires and the simulation. All data recorded will be kept securely in a database. The questionnaires will require multiple-choice responses from participants, and there will also be opportunities to include more qualitative data.

The simulation will present a stimulus, such as a webpage or an email, to the participant, who will decide whether they think the stimulus is genuine or non-genuine. Subsequently, the participant will then justify their decision. The justification will be in the form of options to select from, and participants will then select how confident they are in their decision, either low, medium or high confidence level. The engagement and time taken to respond will be timed.

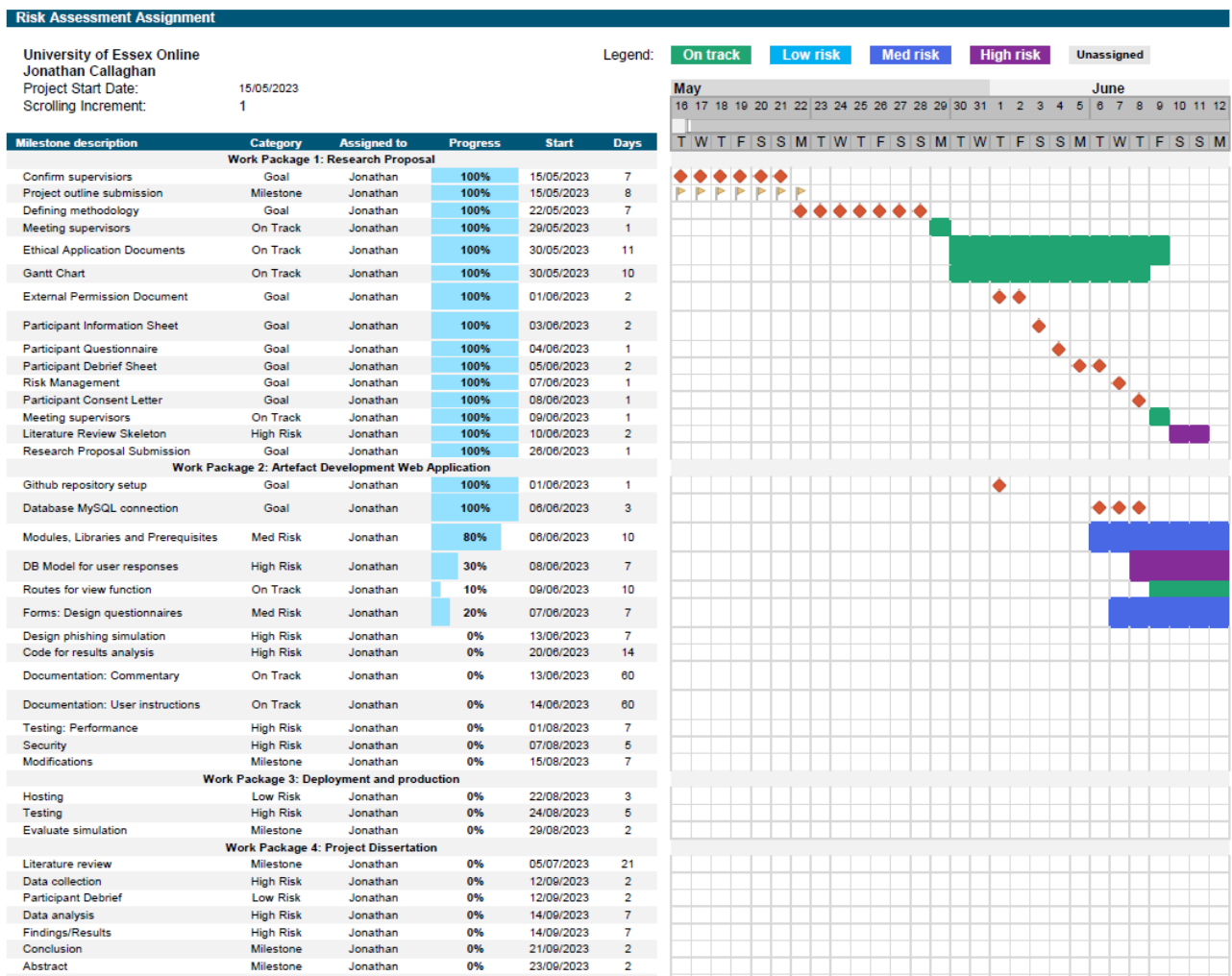
The post-simulation questionnaire will be based on their reflection and cyber awareness since completing the simulation.

Verification and validation will be applied through the design process. The web application will be based on the specified designs with reviews on the development, design document and checking of the code to support verification. Code will be inspected following Python code standards PEP 8 (van Rossum et al., 2013) and Python's Inspect module to objects, modules, classes, methods and functions. In the development stage, testing will occur to ensure the application works correctly.

Validation will occur in the deployment stage to test the simulation to see if the intended outcomes in the design document meet the application's requirements. Further testing can be demonstrated so the application can cope with the sample number of users expected to use the web application.

The validation process will effectively analyse the results from data collected from the questionnaires and simulation to suggest whether this process improved the participants' knowledge and awareness of a phishing attack and identify phishing as a vulnerability.

Timeline (Gantt Chart)



Research area: Cybersecurity Human Factors Cybok 4.2, 4.4, 14.6 (Martin et al., 2021)

Section 2 Ethical approval

1. Consent

The participants will be Secondary school students aged between 11 and 18. Therefore they are classed as vulnerable; to participate, they will require consent from their parent or guardian.

Participants will be presented with a letter of consent, a participant information letter, a parent/guardian information letter and a snapshot information sheet.

The snapshot information sheet is required as a differentiated resource for younger students or lower literacy ability so that participants cannot misunderstand the facets involved in the project that they must undertake. It will also reinforce the main points in the summary of the more detailed information sheet.

The sample of students will be taken from a Hong Kong Secondary School of approximately 60 students, and the school has already been authorised with a signed document to allow this to proceed. The consent letter will indicate the purpose, contacts, process, right to withdraw and signature for consent.

After completing the surveys and the simulation, the participants will be offered a debrief to discuss concerns and confirm that they understand what has occurred. This will eliminate any misconceptions or understandings, particularly from the simulation, as phishing involves deception and the debrief with support mitigation. A debrief information sheet will also be prepared for participants.

2. Right to withdraw

Participation is voluntary, and participants can withdraw from the research at anytime. This is explicitly documented in the Participant Information Sheet, Participant Information Sheet for Parents/Guardians, Participant Information Snapshot Sheet and Letter of Consent. Contact details of the researcher are listed, who can be contacted through numerous methods such as in-person within the school, email, or telephone.

3. Confidentiality

All participants will be provided with a personal identification number so that no personal details such as names or class numbers can reveal the participant's identity. Should any participant wish to withdraw, all information already collected will be destroyed along with the personal identification number. The researcher will provide the personal identification number of the participants. Personal data from participants will be anonymised, and only required data deemed necessary for the project will be collected. Additional data will not be collected. All collected data will be kept until December 2023, after the research project is completed and published.

After the project's successful completion, participants' personal data will not be disclosed to safeguard and protect participants' identities. The group data will be disseminated to a broader audience as part of the findings for presentations; however, individual responses will not be singled out. Participants will be referred to as 'Secondary students in Hong Kong'. Participants may request their own individual results from the phishing simulation but not for anyone else.

4. Harm

Participants will be protected from harm in numerous ways. After risk assessing the project, identifying hazards and control measures, participants will enjoy a safe experience knowing their data and privacy is secured. The informed consent from parents and participants will be explicit through clear communication and documentation of information sheets. The information clarifies the nature of the project, how data will be collected and used and identifying the potential risks involved.

To protect participants, unique identifying numbers will be used instead of using personal information and personal data will be anonymised and encrypted, as detailed in Section 5. As documented in the risk management, whilst the likelihood of a breach is low, the impact would be high if such an event occurred; therefore, security considerations to limited access control, encryption of transit data and personal data with a secure database have been planned. Particular consideration has been given to Hong Kong and GDPR regulations to ensure compliance is adhered to and provide participants access to manage their data, such as to delete it in the case of withdrawal from the project.

Phishing attacks involve victims' deception and can trigger a negative psychological response (Goel et al., 2017). The simulation has documented that it is not real, so there is no misinterpretation that this is an actual phishing event. Therefore, there will be no follow-up actions required by the participants regarding the phishing attempt, and the knowledge that the attempt is not real would not cause stress or anxiety to the participants.

Educating participants about the consequences of misusing the information presented in the simulation will also support the possibility of inadvertent negative learning. Participants will be instructed about the unethical and potentially criminal damages of using learning in a negative manner learned in the phishing

simulation. The debrief following the simulation will reinforce the objectives and eliminate misconceptions to mitigate any risk.

The accessibility and ease of contact to the researcher and staff of the school should any concerns arise are always available. Contact details have been communicated in documentation, and the school institution itself has a strong background in supporting student well-being. The researcher is also a teacher in the school; however, there is an extensive team of staff ranging from tutors to heads of year, educational psychologists, nurses and social workers who are all available to support the participants' physical, emotional and social well-being.

The user experience and interface have also been designed to protect the participants. The web application is designed to use similar features to applications that participants use within the school regularly, such as input boxes, dropdown menus, potentially QR code scanning, downloading additional applications (One-Time-Passcode) is included and a layout similar to platforms already used for lessons. Due to their experience, the participants already possess good fine motor skills for using software applications and can navigate applications effectively.

Participants are protected from potential frustration of use, with a user-friendly interface that is clear to navigate. The school has a policy of Bring-Your-Own-Device (BYOD), and participants can use their device to complete the research tasks that will further support their user experience using a device they are entirely accustomed to.

5. Data access, storage and security

The application system will have two interfaces. One will be for administrators (Researcher) to create and update participants' accounts, and another will be for participants to log in and complete the survey and simulation.

Upon creating a new participant account, the users' email, name, password and gender will be entered. Only the necessary personal data will be collected, such as name, gender, and login details which will be anonymised and encrypted. The data will not be kept longer than deemed necessary and will be deleted after the project has been published (expected December 2023).

There is the possibility of including a one-time passcode generated through a QR code to offer two-factor authentication for the created participant account. However, this is under review as younger participants may find this challenging and have time constraints, as this will be undertaken during the school day. The participants are well versed in using QR codes as they are regularly used in and around the school, so further investigation is required on implementation. The participant data will have a unique identifier to support data minimisation. Passwords will be strengthened using length, upper and lower case and special characters. Hashing will encrypt the password and hashed with salt to mitigate further attacks if the database becomes compromised.

Data will be encrypted in transit of the network using Transport Layer Security (TLS). This protocol supports secure communication between the database where data will be stored and the participant's web browser and server. Using HTTPS for the web application will support this using a Secure Sockets Layer (SSL) public key certificate to authenticate the website's identity to allow an encrypted connection.

The database using MySQL will have secure username and password access with encryption at rest. The third-party provider database service will manage this. Backup and recovery mechanisms will be implemented to provide a secure and reliable database; the third-party provider will automatically run security patches.

As the application will be designed in Python Flask framework, Python libraries will be used to implement the storage and security measures.

Access controls will be in place, and the researcher will be only authorised to access the data. The design of admin and participant accounts will implement authentication and role-based access.

Using Flask, the logging module is available that can support the web application's security. The logging module will offer warnings, errors and debugging information to files to remain informed in case of a potential data breach. In this case, a data breach response plan will be initiated to investigate a potential attack and involve the procedure to notify the affected participants involved.

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 data subjects or authorities (PCPD, 2023a). However, non-binding guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD) advises and encourages notification to PCPD where there would be a risk of harm if data subjects were not informed. In this project, we would follow best practices, inform participants and authorities, and comply with GDPR (PCPD, 2023b).

6. Other issues

The project involves participants classed as vulnerable aged between 11 and 18 years of age. These are high school students from a mixed ability fee-paying government-subsidised school in Hong Kong.

The school operates the formation classes by streaming through entrance tests and attainment grades, and as such, students offered the opportunity to participate will not have Special Educational Needs or Disabilities (SEND) and be fully able to operate the commands and instructions for the research.

The participants can manage fine motor skill coordination using software application features, which will be standard practice. Students at this school regularly participate in research projects electronically and are computer literate. As a registered teacher in Hong Kong and also employed by the school, the researcher will have access to any information that can support the participants who wish to take part and, after gaining clearance from the institution to proceed, will also have staff support.

The school leadership were very keen and excited to hear about the project and the benefits the findings could have for the students at the school and in Hong Kong.



Section 3 Risk Assessment

1. Are there any potential risks, for example, physical, psychological, social, legal or economic, to participants or subjects associated with the proposed research?

YES

Please provide full details of the potential risks and explain what risk management procedures will be put in place to minimise the risks:

- i) Privacy breach: Loss or misuse of personal data. Identification of students from the anonymised data.

Controls: With adequate security and privacy controls in place, the likelihood would be low; however, the impact would be high should a breach occur. Therefore, data handling will require anonymisation through the hash and salted hash, encryption, secure data storage, and only collecting data required for the project. Should a third-party source be used for database storage, then full vetting of security protocols would occur.

- ii) A misinterpretation of the phishing simulation as an actual event: Deception and psychological response. Participants may take action if they think the phishing attempt was real, causing stress or anxiety.

Controls: Clear communication and documentation identify that this does not include real live examples but a simulation for educational purposes. This should also be reiterated in the debrief. Misunderstanding could stem from confusion or stress, so explicit communication should mitigate risk.

- iii) Emotional or psychological distress: Emotional stress or unpleasant worry from phishing

Controls: Documentation and briefing explain that this is not an actual-life event. Whilst the content and participation procedures should not trigger any negative or anxiety response, a support team is dedicated to participants' well-being at any time. They include pastoral teachers, social workers and educational psychologists.

- iv) Inadvertent learning from phishing simulation: Participants could misuse the information presented within the simulation.

Controls: A clear focus on the instructions and communication in the debrief. This should not encompass phishing methods but explicitly identify detection and prevention for educational use. Effective design will minimise risk, and part of the project's goal is that users would make better informed ethical decisions regarding their online lifestyle behaviour.

2. Are there any potential risks to researchers due to undertaking this proposal?

YES

Please provide details and explain what risk management procedures will be implemented to minimise this.

- i) Lone, isolated or out-of-hours working: May need to find an alternative environment to work in a small home area.

Controls: Managing work/family around the schedule. Use the complex facilities in the living block, such as the library. Carefully planning work schedules following the Gantt chart and around full-time work duties.

- ii) Web application: Knowledge and understanding of secure coding development. Inadequate testing of the application. No backup measures and failure to anonymise participant data also complying with data protection and privacy.

Controls: Continuing training and practices applying secure code to minimise the risk of vulnerabilities. Incorporating the tasks to completion in the Gantt chart will support and timeframe. Before deployment and production, thoroughly test the application for security issues or bugs. Create backups of data and recovery plans. Obtain informed consent from participants to ensure compliance with applicable regulations and laws. Also, limiting data collection to what is necessary whilst anonymising participant data.

- iii) Liability and reputation: Potential liability and action from participants due to data breach or simulation misuse. This could also cause damage to the researcher's reputation.

Controls: Strict following of BCS codes of conduct (British Computing Society, 2022), legal and ethical guidelines and following data protection and privacy guidelines for both GDPR (Intersoft Consulting, N.D.) and Hong Kong (PCPD, 2023b).



3. Are there any potential reputational risks to the University of Essex Online due to undertaking this proposal?

NO

Please provide full details and explain what risk management procedures will be implemented to minimise this.

4. Will the research involve individuals below the age of 18 or individuals of 18 years and over with a limited capacity to give informed consent?

YES

(If yes, a Disclosure and Barring Service disclosure (DBS check) may be required. Please attach as part of your application). Give further details of the participants below.

As based in Hong Kong, this is not required as the teacher registration application has its own disclosure process. However, has also received DBS checks previously when employed in the United Kingdom. Has been a teacher since August 2006 and qualified in the United Kingdom.

Attached is the teacher registration certificate for Hong Kong and the qualified teacher status for the United Kingdom.

5. Are there any other ethical issues that have not been addressed which you would wish to bring to our attention?

NO

Give details below:



Section 4 Confirmation Statements

The results of research should benefit society directly or by generally improving knowledge and understanding. I confirm that my research project has a potential benefit. (If you cannot identify a benefit, you must discuss your project with your supervisors to help identify one or adapt your proposal so the study will have an identifiable benefit.)

I confirm that I have read the Research Ethics Policy and the relevant sections of the Research Ethics Procedures and will adhere to these in the conduct of this project.

(These statements must be ticked in the form.)

Signature

Date and Signature space are available in the form.

Attachments

You are required to attach the following documents to this form:

1. An example of your participant information sheet and consent form, if applicable.
2. Consent document from the organisation your research is taking place, if applicable.



References

- Basak, S., Wotto, M. & Bélanger, P. (2018). E-learning, M-learning and D-learning: Conceptual definition and comparative analysis. *E-Learning and Digital Media*, 15, 191-216.
- 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].
- 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.
- Clark, D. (2021). Provision of work for pupils learning from home at schools in England 2021. Available from: <https://www.statista.com/statistics/1266587/online-learning-methods-at-schools-england/> [Accessed 26 March 2023].
- Dawson, C. W. (2009). *Projects in Computing and Information Systems: A Student's Guide*. Pearson Prentice Hall.
- 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.
- Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L. F. & Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.*, 28, (6): Article 43.



Duffin, E. (2022). Share of U.S. K-12 students who use digital learning tools daily by level 2019.

Available from: <https://www.statista.com/statistics/1076292/share-k-12-students-us-who-use-digital-learning-tools-daily-level/> [Accessed 26 March 2023].

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

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

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\).](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].

Hong Kong Computer Emergency Response Team Coordination Centre. (2021). Annual Report.

Available from:

https://www.hkcert.org/f/press_center/909710/910908/HKCERT%20Annual%20Report%202021.pdf [Accessed 20 June 2023].

Intersoft Consulting. (N.D.). GDPR. Available from: <https://gdpr-info.eu/> [Accessed 22 January 2022].

Irwin, L. (2023). The 5 Most Common Types of Phishing Attack. Available from:

<https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack> [Accessed 26 March 2023].

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

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3, (1): 9.

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.

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].

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.

Pcpd. (2023a). Data Breach Notification. Available from:

https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html [Accessed 22 June 2023].



Pcpd. (2023b). EU General Data Protection Regulation (GDPR) and Hong Kong. Available from:

https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html [Accessed 22 June 2023].

Qualtrics. (2023). An introduction to t-test theory for surveys. Available from:

[https://www.qualtrics.com/uk/experience-management/research/t-](https://www.qualtrics.com/uk/experience-management/research/t-test/#:~:text=What%20is%20a%20t%2Dtest,mean%20and%20a%20standard%20value)

[test/#:~:text=What%20is%20a%20t%2Dtest,mean%20and%20a%20standard%20value](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].

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

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.

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

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 20 June 2023].

The Government of the Hong Kong Special Administrative Region. (2023). Government lowers response level in relation to COVID-19 epidemic to Alert level. Available from:

<https://www.info.gov.hk/gia/general/202305/30/P2023053000552.htm> [Accessed 19 June 2023].

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.

Van Rossum, G., Warsaw, B. & Coghlan, N. (2013). Python Developer's Guide. Available from: <https://www.python.org/dev/peps/pep-0008/#overriding-principle%20336> [Accessed 2 September 2021].

Wheelan, J. (2013). *Naked Statistics: Stripping the Dread from the Data*. New York, W.W. Norton.

Zorlu, E. (2022). An Examination of the Relationship between College Students' Cyberbullying Awareness and Ability to Ensure their Personal Cybersecurity. *Journal of Learning and Teaching in Digital Age*.



Appendices

1.1 Letter of consent

1.2 Participant Information Sheet

1.3 Participant Snapshot Information Sheet

1.4 Parent/Guardian Information Sheet

1.5 Participant Debrief Sheet

1.6 Participant Questionnaire

1.7 External Approval Form

1.8 Teacher Registration Documents



1.1 Letter of consent

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

Signed *Date*

Signature:

Name of Parent / Guardian*:

Date:



1.2 Participant Information Sheet

Participant information sheet (Detailed version)

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

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

Take time to decide if you want to participate in this study. Before you take part, it is essential to ensure that you 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 would like to obtain more information or have any concerns about this research project, please contact the researcher at jonathan.callaghan@yhkcc.edu.hk **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 offer you (the student) an assessment of your cybersecurity awareness concerning phishing attempts and empower you to make informed choices to manage your 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 involvement in this research will take one session of approximately 10-20 minutes to complete.

You will complete a questionnaire assessing your cyber awareness knowledge and understanding as a participant. Then you will complete a phishing simulation exercise that will not be real or impact real life as it is solely for research purposes.

During the simulation, you will view a stimulus, such as a webpage or an email and decide whether you thought the stimulus was genuine. Following, you will provide a reason/justification for that decision. Next, you will select a score of your confidence in making that decision, whether low, medium or high confidence. Your response will be timed. You then will answer further questions from the questionnaire to reflect on your 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, 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.

What will you have to do?

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

You will be provided with a website to register a username and password which will be provided to you. 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 participants will have time to complete it.

You will then be provided with three tasks:

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

You 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 learning and management of your online presence and behaviour. It may also provide a current assessment of your knowledge concerning the topic. You 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 objectives. You may find this process particularly useful to apply your knowledge practically rather than only theoretical lessons in Personal, Social, and Health Education (PSHE) lessons.

The dangers of participation – Low risk

The concerns are that you (the student) 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 possibly happen when you are online. 'Not a live environment' suggests that the situation is not real and your responses will not matter in real life. It is essential to understand that the methods used in the simulation should not be shared or have opportunities to be misused in the future, which could result in criminal activity.

Data from the questionnaire will be anonymised, so you will be provided with a unique identification number instead of using your personal data. 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.



Withdrawal from participation

The research is voluntary, and you can withdraw from the research at any time. All information related to you 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.

There is no intention to cause emotional distress through your participation in this project; however, if you do, please seek support from the contact details below.

We have the Student Well-being Team on campus to support your needs, including social workers and educational psychologists located in the Well-being Office.

Jonathan Callaghan – jonathan.callaghan@yhkcc.edu.hk

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 your individual responses will not be singled out. You will be referred to as 'Secondary students in Hong Kong'.

If you would like to receive your 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 jonathan.callaghan@yhkcc.edu.hk or telephone number 29883035.

Thank you for your interest in participating in this study.



1.3 Participant Snapshot 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 jonathan.callaghan@yhkcc.edu.hk

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/technology_crime.htm

Cyber Youth Programme

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



1.4 Parent/Guardian 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 jonathan.callaghan@yhkcc.edu.hk **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.

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:

- 4) A questionnaire to self-assess cybersecurity awareness.
- 5) 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.
- 6) 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.

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.

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 Well-being Team on campus to support needs, including social workers and educational psychologists in the Well-being Office.

Jonathan Callaghan – jonathan.callaghan@yhkcc.edu.hk

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 jonathan.callaghan@yhkcc.edu.hk or telephone number 29883035.

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



1.5 Participant Debrief Sheet

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 jonathan.callaghan@yhkcc.edu.hk, who will process the request. Please be aware that a summary will be provided.

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**](mailto: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 Well-being 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**](https://www.cybersecurity.hk/en/learning-scam.php)

CyberSec Hub [**https://cyberhub.hk/**](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 jonathan.callaghan@yhkcc.edu.hk

Thank you again for your taking part in this research.



1.6 Participant Questionnaire

Participant Questionnaire

Pre simulation

1) What gender do you identify as?

Male

Female

Prefer not to say

2) How old are you?

11

12

13

14

15

16

17

18

19

3) Have you ever received any form of cyber awareness safety learning or training?

Yes

No

4) Do you know what phishing is?

Yes



No

- 5) Have you ever received a message, email, or any other means that you suspected was a phishing attempt?

Yes

No

- 6) How confidently could you distinguish between genuine and phishing emails on a scale of 1-5 (1=Low Confidence, 5=Very Confident)?

- 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



Post simulation

- 1) After completing the phishing simulation, has this increased your awareness and understanding of phishing?

Yes

No

- 2) How confidently could you distinguish between genuine and phishing emails on a scale of 1-5 (1=Low Confidence, 5=Very Confident)?

- 3) From the phishing simulation, what did you find the most helpful?

Identifying potential phishing emails

Handling and managing the 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

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=Very effective), how effective was the simulation in educating you on phishing?

1

2

3

4

5

7) Can you 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



1.7 External Approval Form



YMCA of Hong Kong Christian College

2 Chung Yat Street, Tung Chung, N.T.

Tel: 2988 8123 Fax: 2988 2000

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 YMCA of Hong Kong Christian College 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,

Diana Lo

Principal





1.8 Teacher Registration Document

表格9
FORM 9

教育條例
EDUCATION ORDINANCE
(第279章)
(Chapter 279)

檢定教員證明書
CERTIFICATE OF REGISTRATION AS A TEACHER

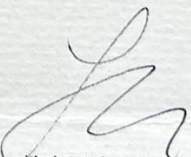
註冊編號
(Registration Number: R304404)

茲證明
This is to certify that

CALLAGHAN, JONATHAN JOSEPH

已根據《教育條例》第45(1)條註冊為教員。
is registered as a teacher under Section 45(1) of the Education Ordinance.




教育局常任秘書長
(劉彩珠代行)
(Ms Gregor C C LAU)
for Permanent Secretary for Education

香港特別行政區 二零一八年七月二十六日
Hong Kong Special Administrative Region 26 July 2018



Cyngor Addysgu Cyffredinol Cymru
General Teaching Council for Wales

Qualified Teacher Status Statws Athro Cymwys

This is to certify that:
Tystia hyn fod:

Jonathan Joseph Callaghan

Teacher reference number:
Rhif cyfeirnod athro:

0577815

has attained qualified teacher status (QTS) to teach in Wales
wedi ennill statws athro cymwys (SAC) i addysgu yng Nghymru

Date of QTS:
Dyddiad SAC:

01 August 2006
01 Awst 2006

Congratulations and best wishes for your future career
Llongyfarchiadau a dymuniadau gorau ar gyfer eich gyrfa yn y dyfodol

Mai Davies
Chairman, General Teaching Council for Wales
Cadeirydd, Cyngor Addysgu Cyffredinol Cymru