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 with 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 using.

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.

Safeguarding:

Consent from participants and parents/guardians.

Unique identifiers for participants to protect personal data.

The security protocols mentioned above will support compliance with GDPR.

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.

Safeguarding:

Professional conduct.

Debrief session and information sheet.

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.

Safeguarding:

Members of staff and well being staff available to support participants.

Safe environment, good lighting, glass doors, wall and windows for transparent viewing.

Complaint and reporting procedure for all stakeholders involved to raise if any concerns.

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.

Safeguarding:

Professional conduct.

Debrief session and information sheet.

v) Development process: Limited or poor user experience:

Usability of the web application

Controls: Test the web application and usability. Gain feedback on its user and improve. Include on the Gantt chart.

Safeguarding:

Consent to support testing.

Safe environment.

Emergency procedures incase of any failure or emergency response.

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).

iii) Development process: Testing- Failures or inadequate testing causes vulnerabilities and bugs.

Series of tests such as unit, feature, integration and performance testing. Usability, functionality and security penetration tests will also need planning.

Safeguarding:

Compliance with all laws and regulations.

Contingency plan if project delays occur with realistic deadlines.

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:

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].

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

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

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].