Jonathan Callaghan University of Essex ID: 12686209
CYSPROJ_PCOM7E May 2023

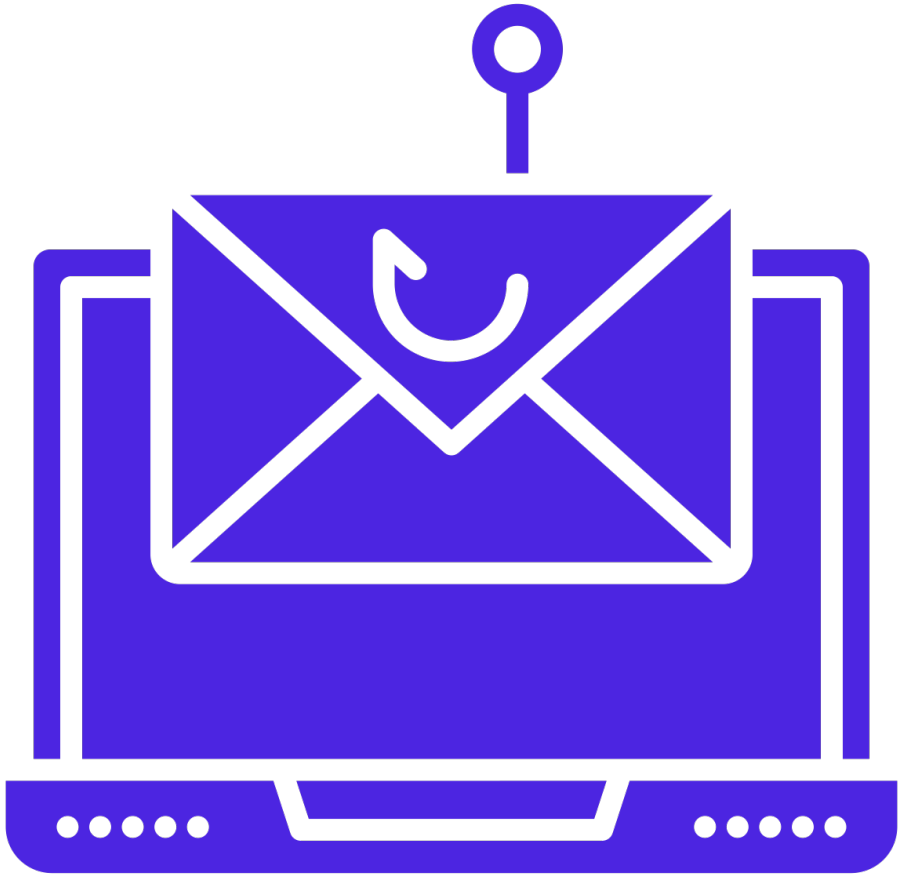



Photo by Jacob Lund from Noun Project

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

Artefact: Phishing simulation

Artefact overview and objectives

Research question:

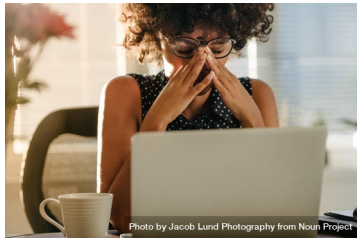
To what extent can cybersecurity awareness empower secondary school students to mitigate phishing attempts during e-learning?

Aim: To produce a phishing simulation to assess students' awareness of phishing emails as a training tool when undertaking e-learning.

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

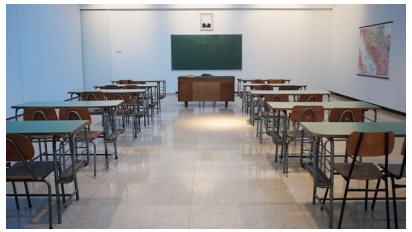
- Hong Kong pandemic Jan 2020-May 2023
- E-learning can be defined as integrating technology in schools providing interactive experiences (Rodrigues et al., 2019)
- Schools ill-prepared for e-learning adoption (Cheung, 2023)

- E-learning flexibility for platforms and integration
- Students good phishing knowledge, usability hinders practices (Nicholson et al., 2021)



- Stakeholder online competency issues (Shaikh et al., 2023)
- Students overestimate confidence and abilities to mitigate (Diaz et al., 2020)

- 62% phishing training for staff and less for students (Gov.UK, 2023)
- Limited understanding of the physical, emotional and social repercussions



- HK Schools targeted by phishing attacks (Ho, 2020)
- Phishing accounted for 48% of all attacks, increase of 7% by 2021 (HKCERTCC, 2021)
- Vulnerabilities in security (password policies, outdated software, human error)

Background and context

Discussion of protective measures

Simulation

- Increases cyber awareness (Chowdhury & Gkioulos, 2021)
- Safe and controlled environment (Sağlam et al., 2023)
- Not offering real life scenarios

Security measures

- Email filtering
- Multi-factor authentication
- Training
- Domain blocking

Gamification

- Increase knowledge (Chau et al., 2019)
- Concerns over diversification and higher order understanding
  Time consuming
- Concerns over preparation for real life threat

Machine Learning / Artificial Intelligence

- Comprehensive strategy for identifying phishing (Seth & Damle, 2022)
- Classify phishing attacks (Bagui et al., 2019)
- Lack of provisions in schools

Self-efficacy

- Empowers learners and protect personal details (Lee et al., 2023)
- Breed overconfidence (Diaz et al., 2020)
- School curriculums inadequate but could support society (Henshaw, 2023)

Web application with phishing simulation

Vulnerable group

Ability and needs

Deception

Environment

Support

Methodology

Preparation

- Approval from the school (English medium school, diverse cultural backgrounds)
- Participation offered to 897 mixed ability 11-18 year old secondary school students
- Video advertisement in year assemblies
- Information sheets
- Literature review

Web application

- Development: Research and design
- Python Flask web application coding development
- Database development and research cloud database
- Testing: Pytest – Functional and unit testing (58 test cases for users, features, data responses) Pylint testing.
- Deployment: Integrated third-party provider for hosting and cloud database

Data collection

- Consent forms distributed and returned signed by parent/guardian
- Three scheduled time slots for students to attend
- School wellbeing team supported for intervention
- Mixed-method research approach through the web application

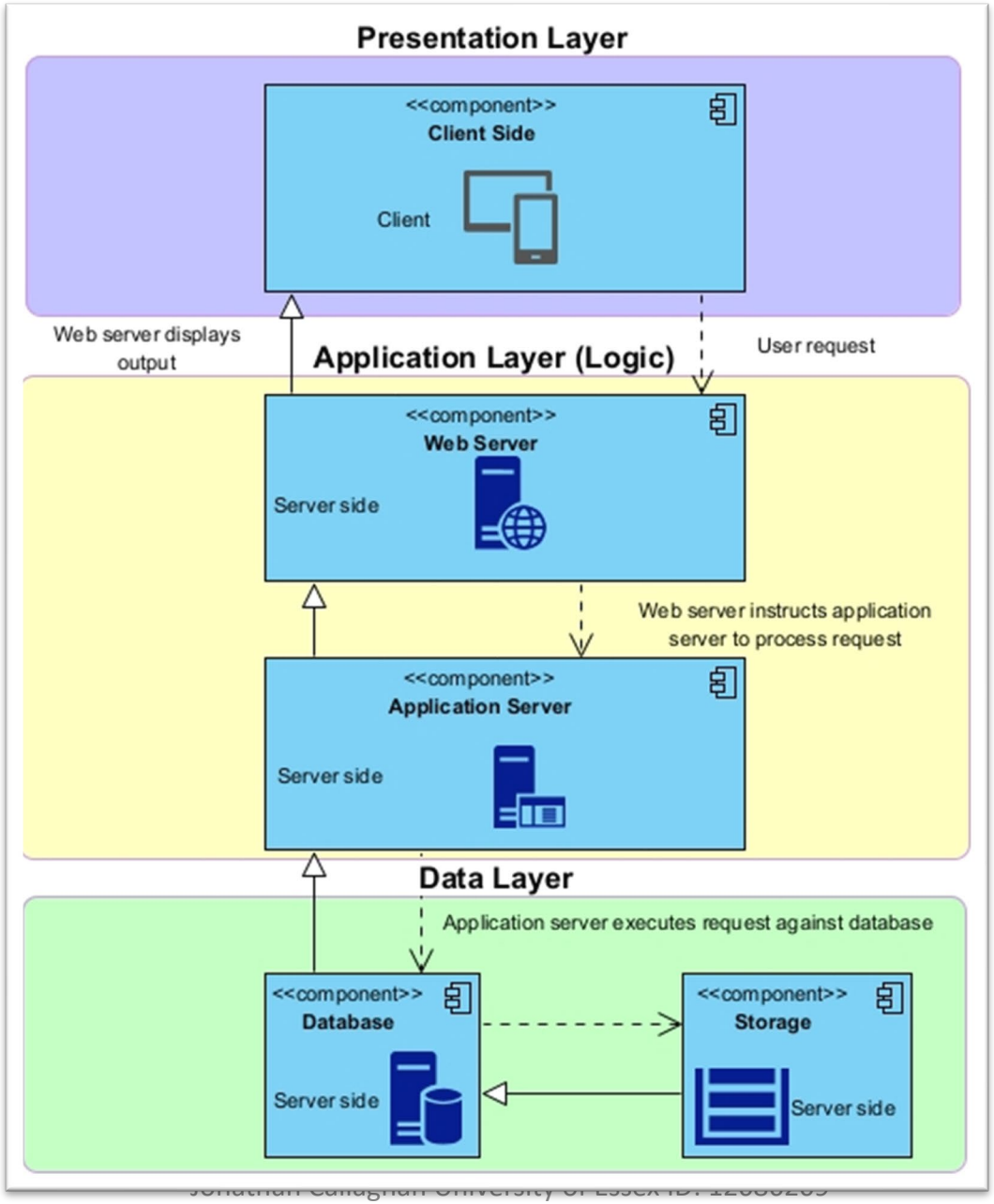
Results

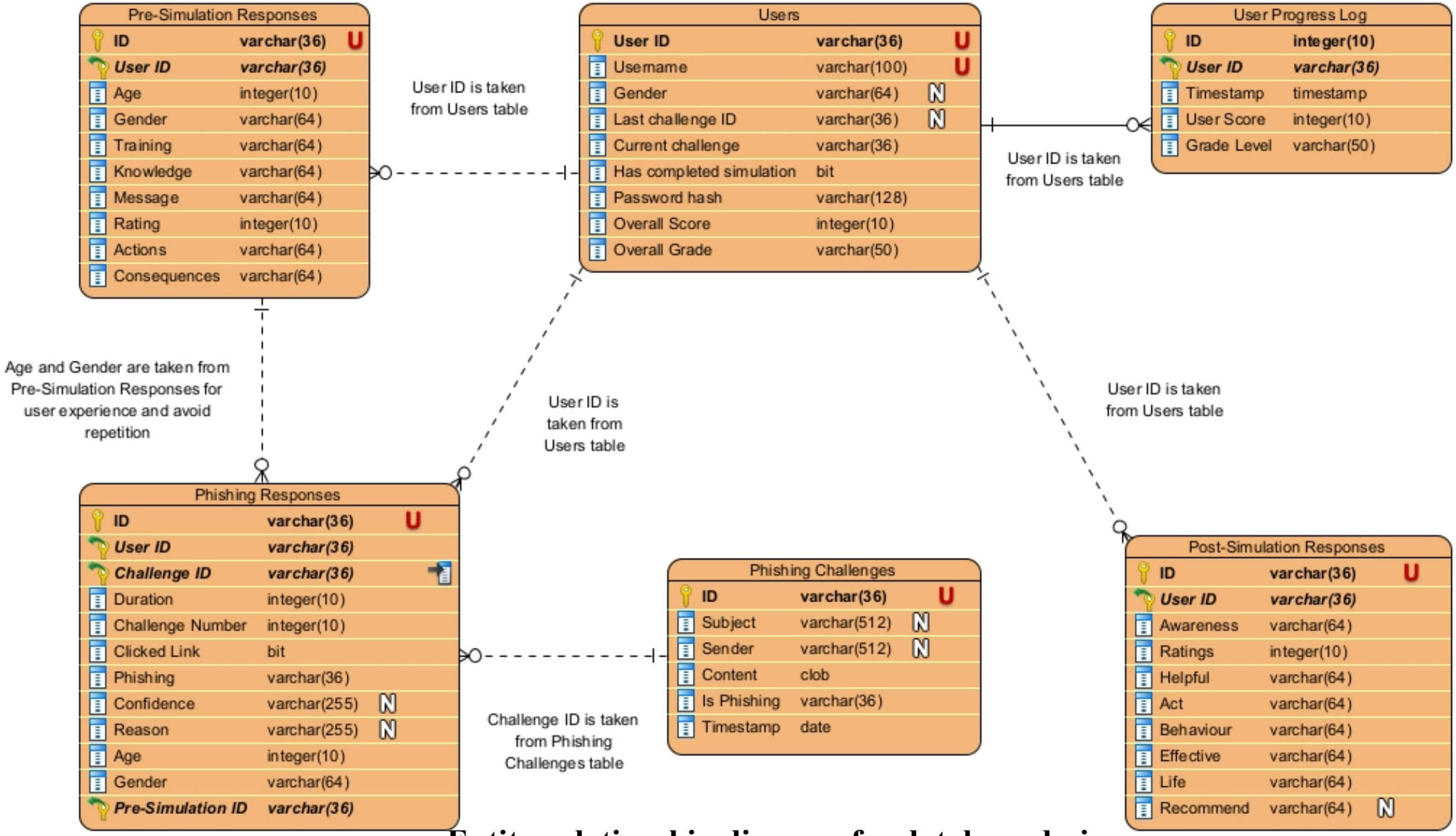
- Data analysis (Descriptive and in-depth)
- Findings
- Dissertation

Artefact

- Python flask web application
- Training tool
- Aimed to be used prior to e-learning
- Questionnaires (Before and after the simulation)
- Simulation – 6 email challenges to identify, user confidence rating and optionally provide reason for decision.
- User score and grade level with tips for phishing awareness
- Progress log for users to attempt in the future

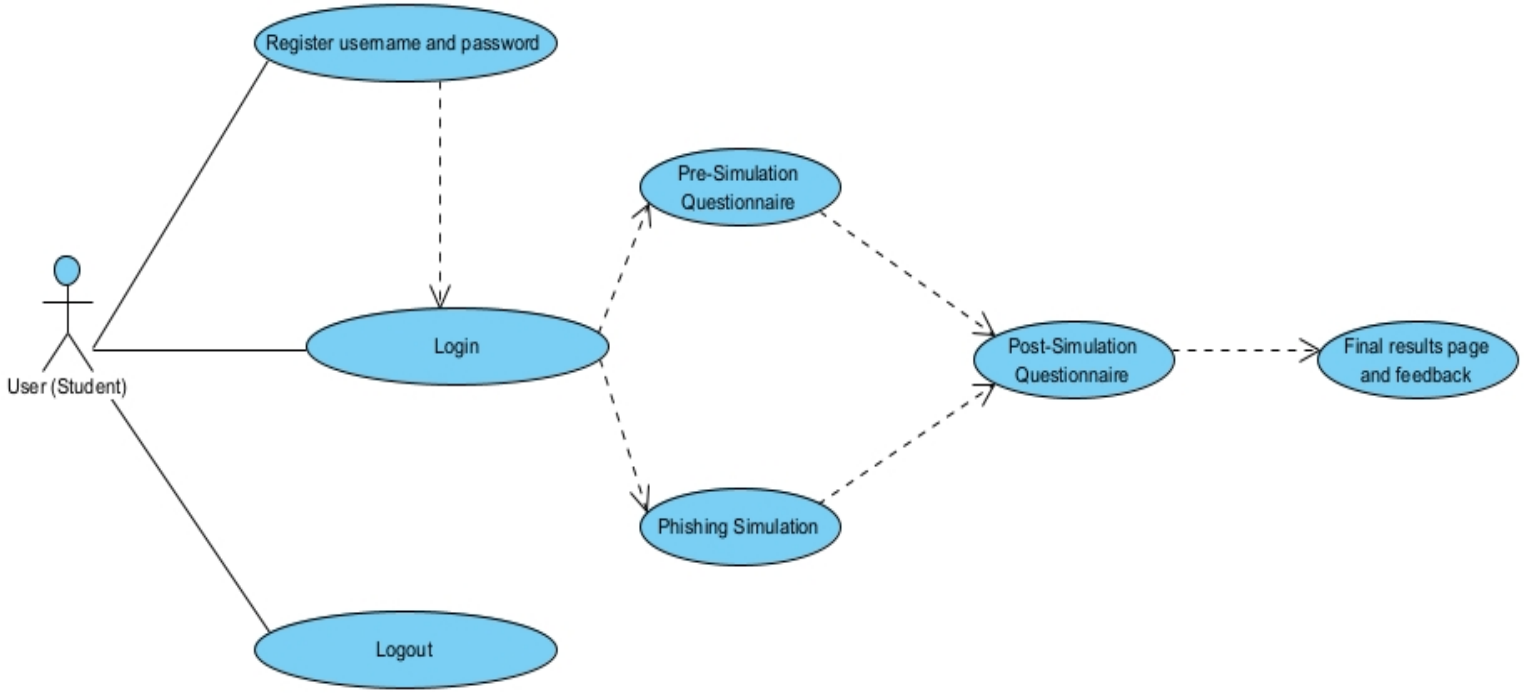
Overview of three-tier architecture diagram



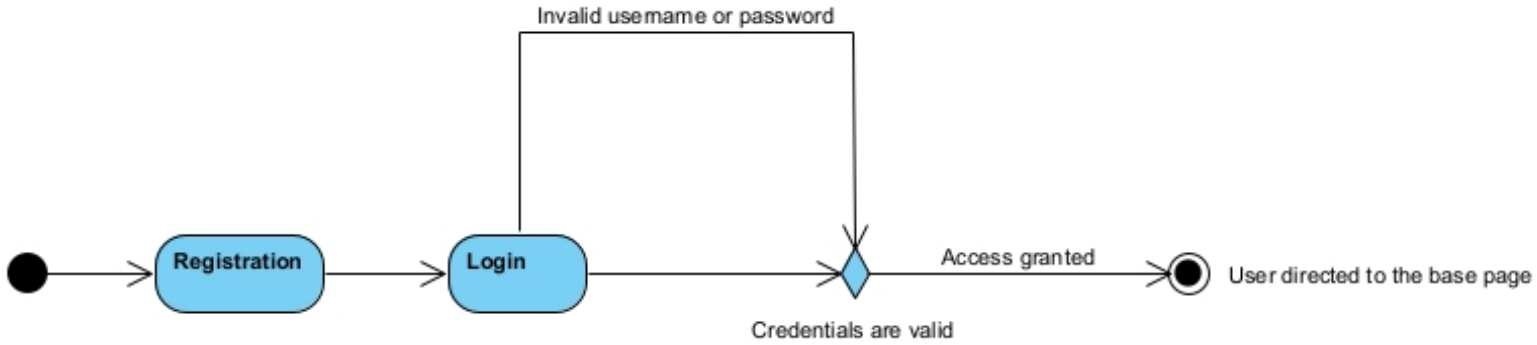


Entity-relationship diagram for database design

Use case diagram for user common functions

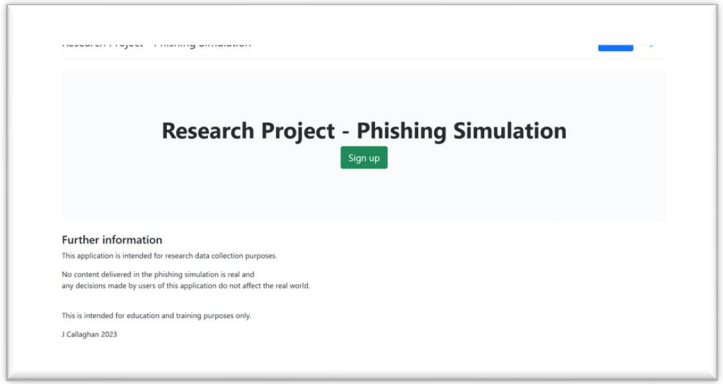


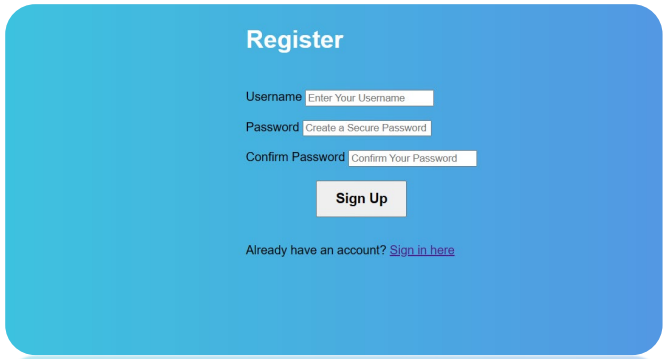
Activity diagram of user login



Demonstration

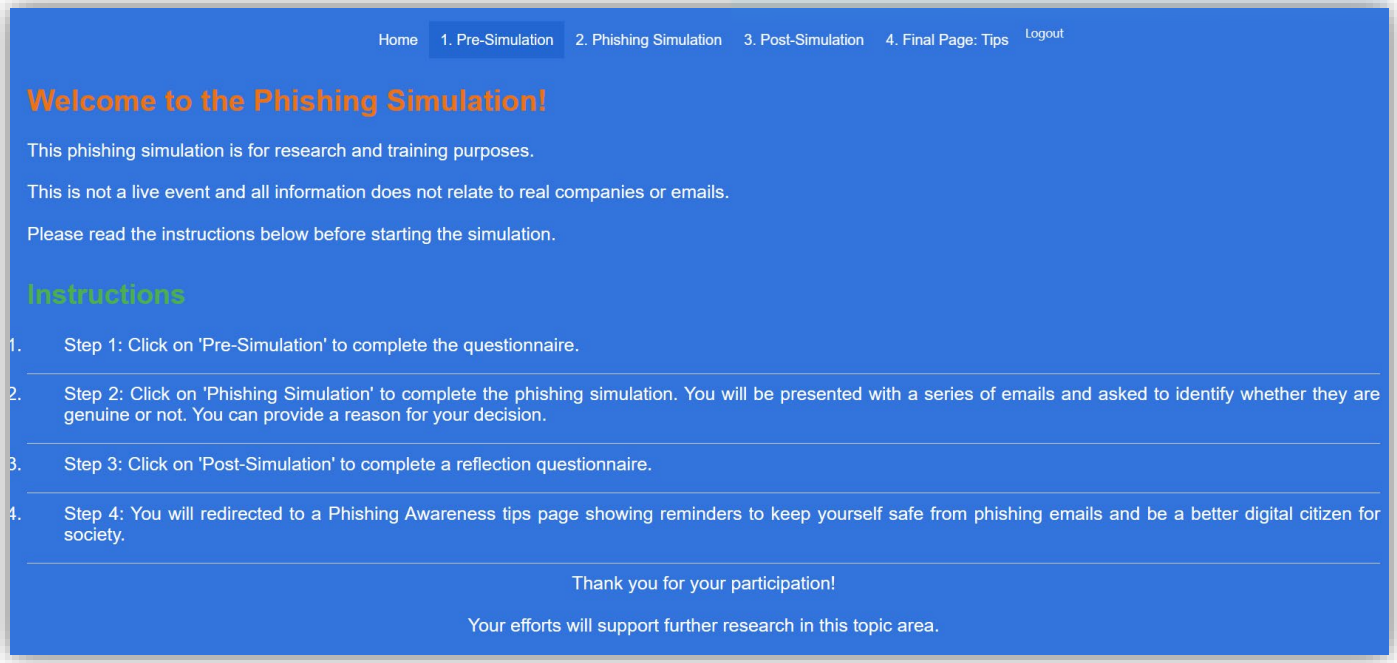
(This can be live)





- User personal data was limited to username, age, gender with universally unique identifiers (UUIDs).

- Passwords were hashed using werkzeug.security library before database storage.



Pre-Simulation Questionnaire

Question 1: What is your age?

30

Question 2: What is your gender?
(As per your national identity document)

- (●) Male
- ( ) Female

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

No, I have never been trained / had any learning about it.

Question 4: Do you know what phishing is?

Yes, I do know what phishing is.

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

Yes, I have received a suspected phishing attempt.

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

- ( ) Low confidence
- ( ) Developing confidence
- (●) Fairly confident
- ( ) Strong confidence
- ( ) Very strong confidence

Question 7: How would you act if you received an email and suspected it to be malicious?

Unsure

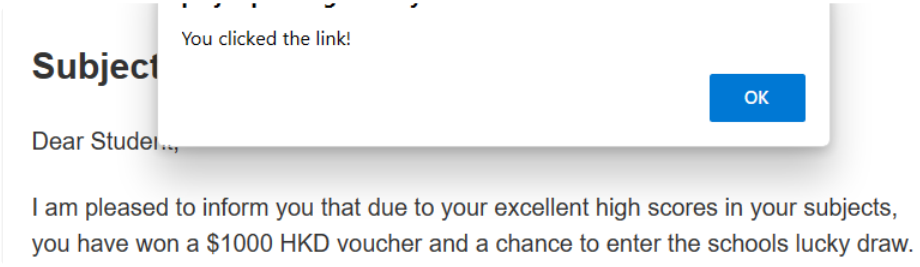
Question 8: Do you fully understand the potential consequences of being a victim of a phishing attempt, such as clicking on a URL website link from an unknown sender?

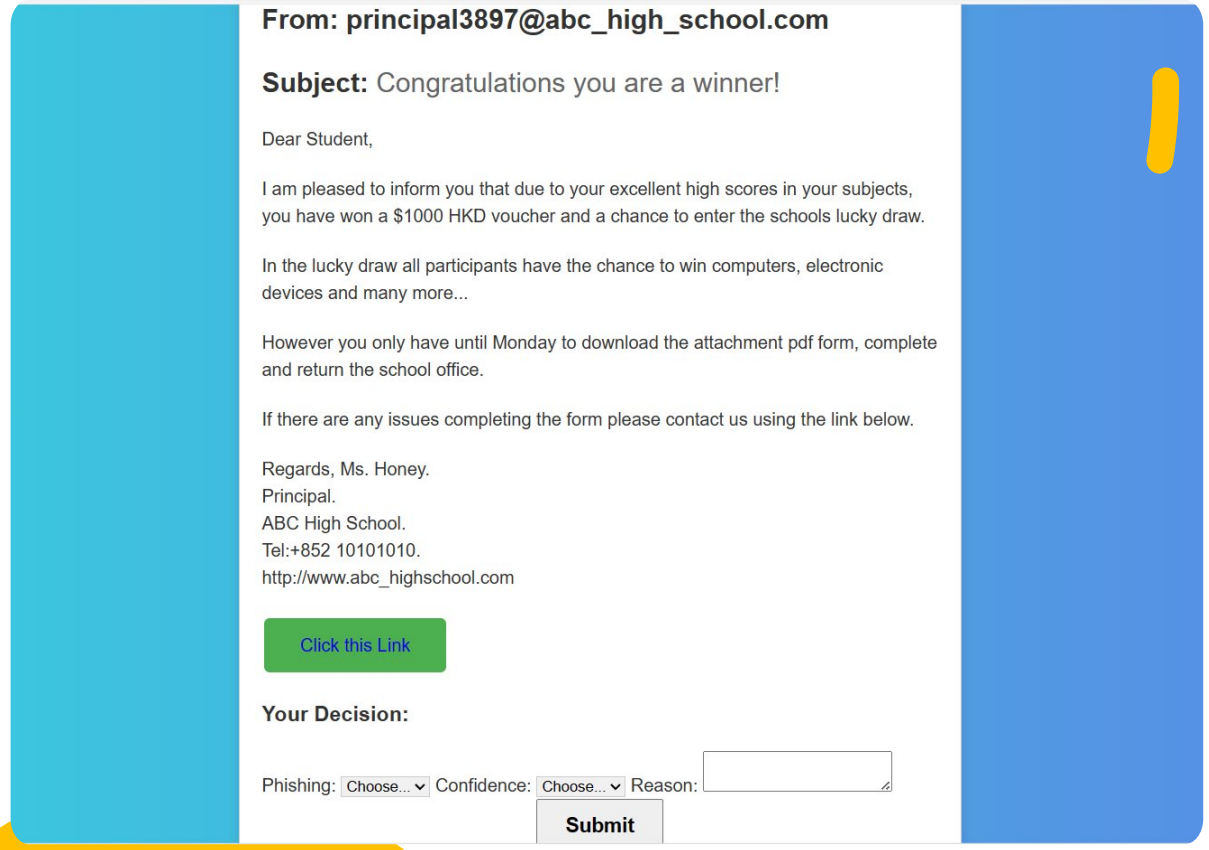
Partly understand

Submit

Questionnaire 1

- Collected:
- Age and gender
- Cyber awareness / Experience
- Knowledge of phishing
- Confidence in managing phishing





Example email challenge

- Spear phishing strategies aimed at students
- Relevant and relatable emails
- URL links are not active but record clicks
- NIST Phish Scale considered in design for cues and alignment (Dawkins & Jacobs, 2023)

Post-Simulation Questionnaire

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

Yes

Question 2: How confidently do you think you could distinguish between genuine and phishing emails in the simulation on a scale of 1-5 (1=Low Confidence, 5=Very strong confidence)?

- ○ Low confidence
- ○ Developing confidence
- ○ Fairly confident
- ◉ Strong confidence
- ○ Very strong confidence

Question 3: From the phishing simulation, what did you find the most helpful?

Identifying potential phishing emails

Question 4: How would you now act if you received an email and suspected it to be malicious?

Report the email

Question 5: After completing the simulation, will your online behaviour change? (verifying sender details, cautious of URL clicking)

Yes, I will be more attentive to what I click on or view.

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

- ○ Not effective at all
- ○ Somewhat effective
- ◉ Moderately effective
- ○ Very effective
- ○ Extremely effective

Question 9: Would you be able to apply the information learned from this exercise to real life?

Yes

Question 10: Would you recommend this phishing exercise to others to support their cyber awareness of phishing?

Yes

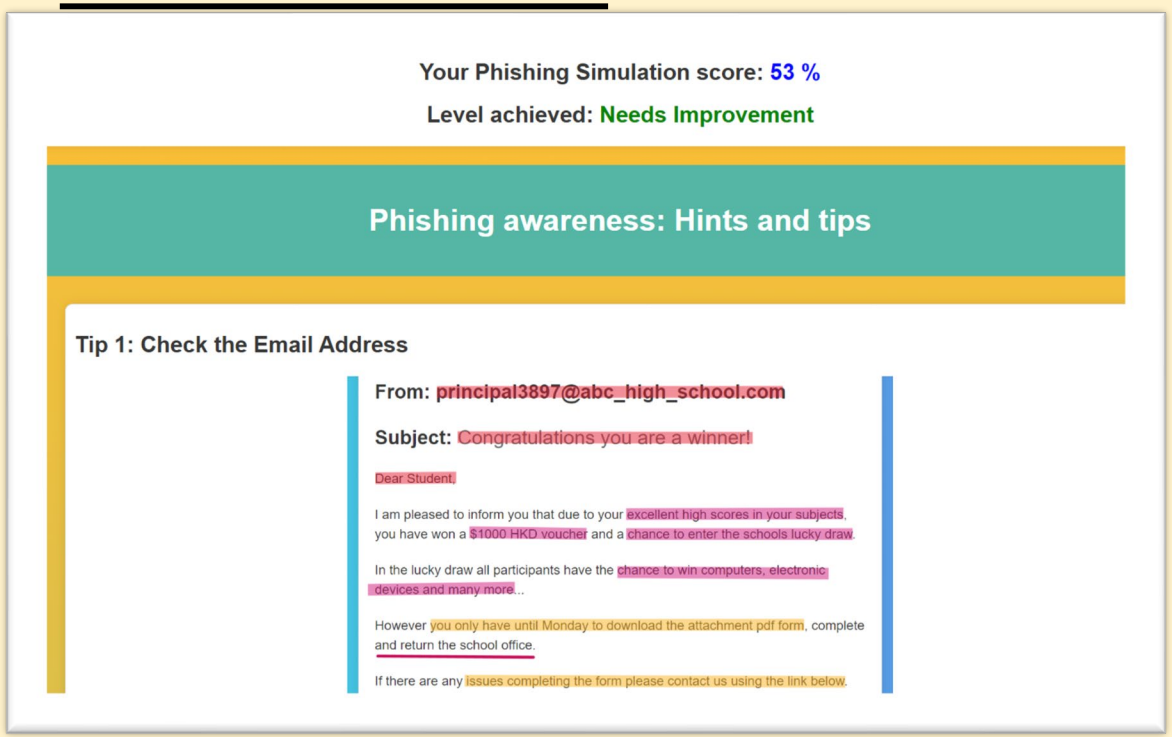
Submit

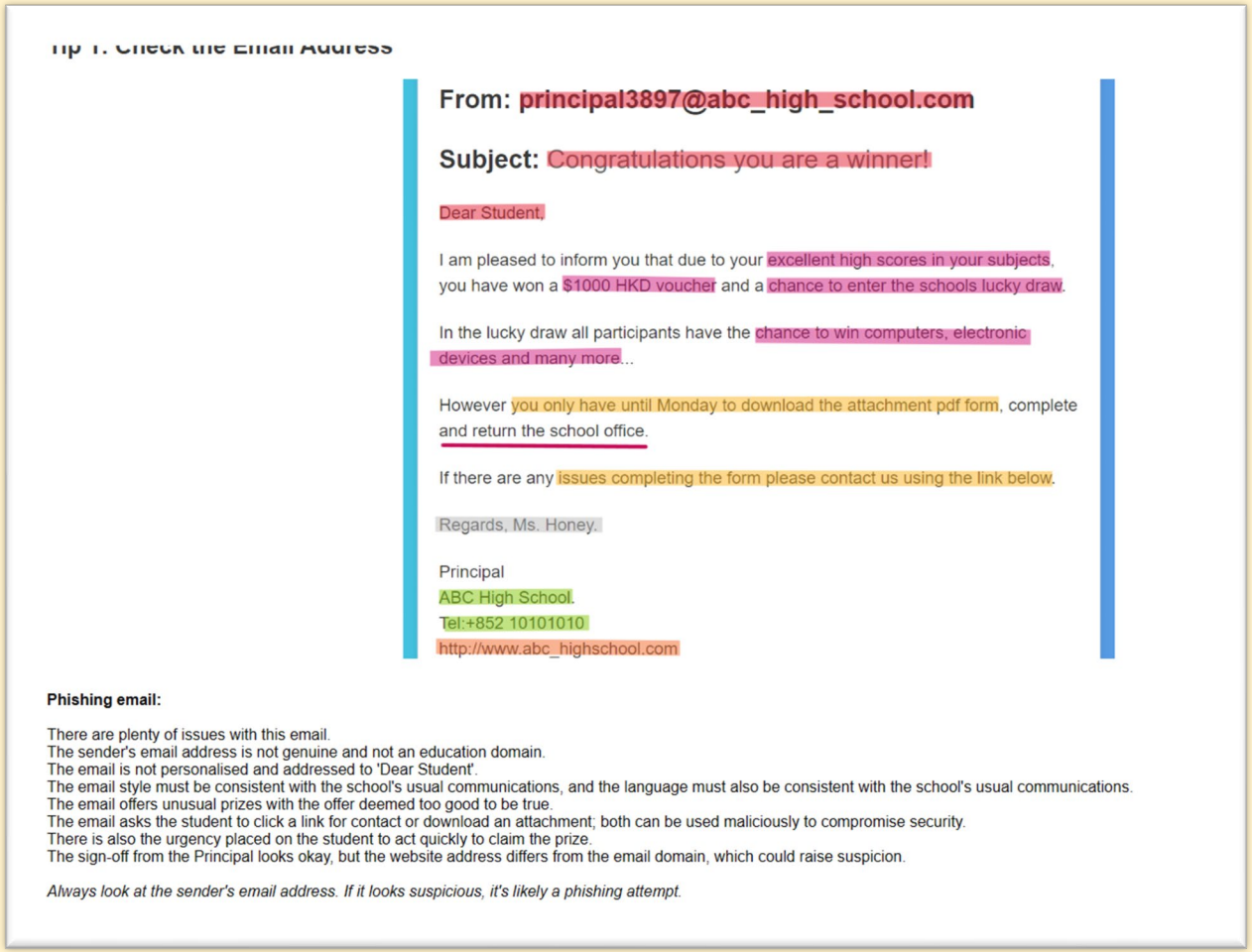
Questionnaire 2

Reflection:

- Cyber awareness and phishing
- Potential behaviour changes
- Effectiveness of the simulation tool
- Application to real life
- Recommendation

User results





Grading scale based on the school criteria levels.

All scores recorded in a progress log with a breakdown for each challenge as well as overall score.

Colour highlighting to identify cues and explanation to support the phishing/genuine email.

Engagement

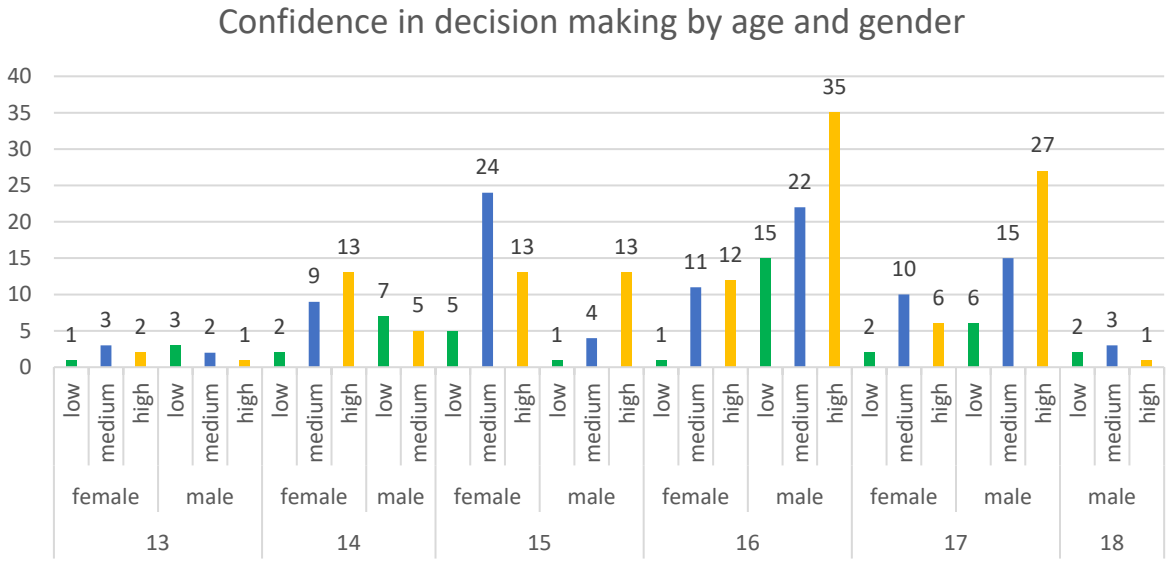
Strategies:

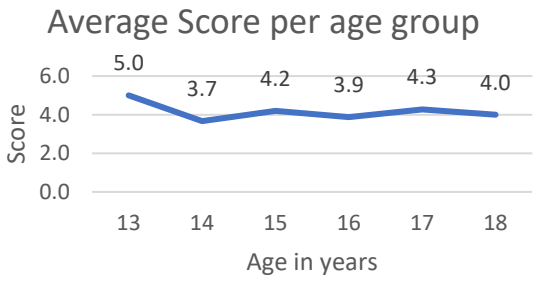
- Accessibility for younger learners simple but appropriately challenged
- Low stakes
- Input features: Radio buttons, scale ratings, drop down menus, text box.
- Students are familiar with these features.
- Application of cues as visual indicators – Observational. Higher cues higher identification.
- Emails similar to communications students may receive - Alignment (Canham, 2022)
- Click rate reduced considerably throughout
- Participants sensed familiarity in genuine emails
- The feedback page provided informative explanations to consider for a more informed digital lifestyle

Analysis

Effectiveness and impact

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





Participants	46	
Statistic	Age	Overall Score
Mean (Average)	15.7	53.7
Standard Deviation	1.2	9.6
Minimum	13	35
Maximum	18	70
Range	5	35

- Males perceived themselves as more knowledgeable despite females averaging higher scores. Males also took longer to answer the challenges.
- Over confidence does not always lead to practical application.

Analysis

Effectiveness and impact

Content alignment – familiarity, past experience, logical process

"I have seen this in the past"

"Email and domain appear real. Alternative contact info given, as well as instructions on how to claim that do not require you to click the link such as claiming at the office. Also value sum is small and realistic therefore not too good to be true"

"In my experience, I have received emails from the school about the book coupon that looked like this"

Misled – judged details as credible

"It is from a principal of the school and all the info is given including her phone no . and the reason for the mail"

"As its a genuine email from your own high school it doesn't seem like they would phish you"

"States the Principal's name which wouldn't have been there if it was a phishing email"

Content cues – exaggerated content, instinctive reasoning

"Not personalised"

"The email username is principal2897, I don't think an actual principal would use that name"

"There's no way the school would give me free money"

Lack of cyber awareness

"It doesn't seem suspicious"

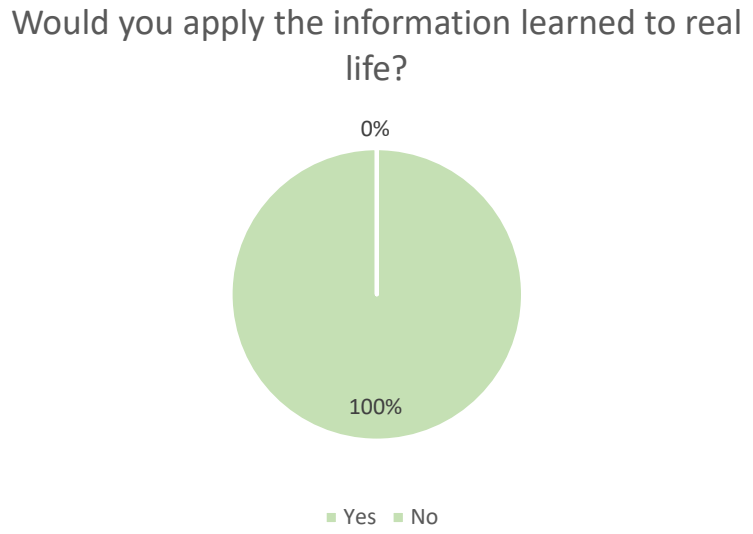
"I have no experience with these sort of emails"

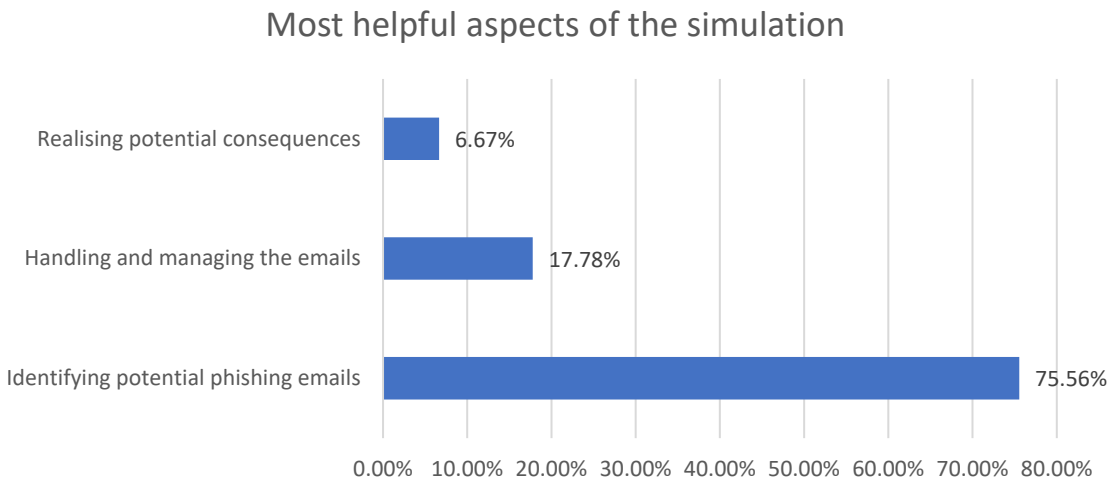
"Looks as to be trustworthy since it doesn't ask for anything yet, not sure though"

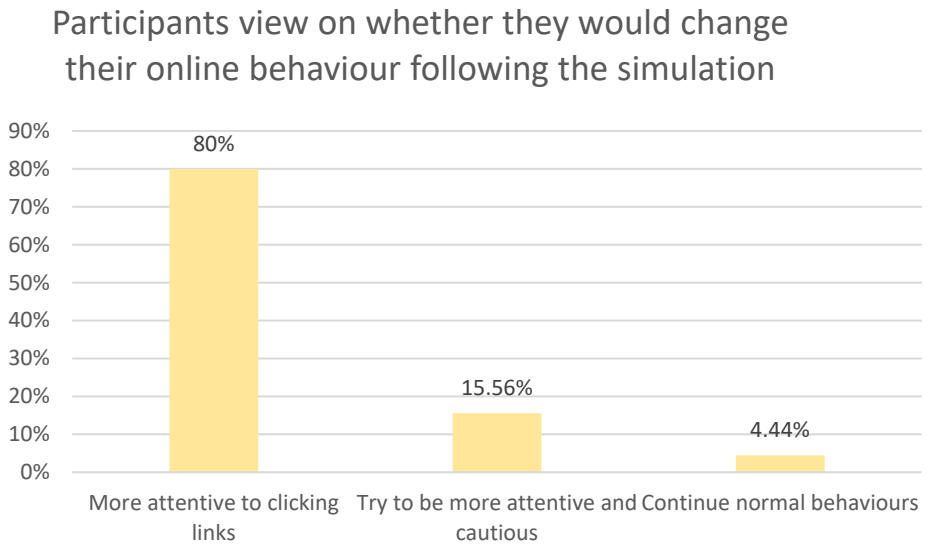
Analysis

Effectiveness and impact

- Students suggested they would aim to apply the knowledge of the simulation.
- Students suggest they would also act with greater attention to email content.







Evaluation

Limitations

- Participation range and sample size
- Due to the sample some relationships can be deemed statistically insignificant
- Variety of email challenges
- Consequences of clicking a link
- Limited opportunities for qualitative data particularly in questionnaires
- Types of phishing
- Interactivity and display of the base page

Future improvements

- Large sample size
- Study across academic student life
- Global study
- Compare other methods (workshops / self-assessments / etc)
- Gender approaches to learning
- Periodic training
- Email challenges to involve greater critical thinking
- Improved features: Password change, gamification, mock consequences, scenario/lifestyle impacts, multi-factor authentication, login rate limiting
- Base page display and interface improvements
- Compatibility for mobile phone devices
- Future simulation tests include a reflection on behavioural change

Conclusion

Findings reveal that greater cyber awareness / training is needed.

Low click rates and high accuracy identification suggests students do have cyber awareness to mitigate phishing.

Inconsistency in cue identification.

Overconfidence and gender approaches.

Students enjoyed the simulation method.

Artefact simulation provides opportunity for differentiated learning and monitoring of progress.

References and image credits

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

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.

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

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

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

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

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

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.

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.

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].

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.

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

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

1. https://thenounproject.com/lakoneicon/
2. College students using laptop while sitting at table by Jacob Lund Photography from Noun Project (CC BY-NC-ND 2.0)
3. Photo by Pop & Zebra on Unsplash
4. https://thenounproject.com/icon/online-learning-6262515/
5. Stressed woman working at her desk by Jacob Lund Photography from Noun Project (CC BY-NC-ND 2.0)
6. https://thenounproject.com/icon/internet-3337510/
7. https://thenounproject.com/icon/phishing-6088107/
8. Photo by John Schnobrich on Unsplash
9. https://thenounproject.com/icon/sample-5262534/
10. https://thenounproject.com/icon/gender-975404/