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. Hong Kong was unique in its strategy to manage the virus; Schools were ill-prepared for the rapid shift in methodology to deliver curriculums to students online due to the suspension of the regular school day (Cheung, 2023).

Students and staff were expected to stay home, and lessons would be delivered remotely; the connection between technology integration and teacher professional development was not fully established, and remote teaching was brought about due to parental pressure (Cheung, 2023).

During this period, teachers were subjected to disruption and cyber attacks. This came in the form of phishing attempts. Teaching staff could be emailed false website links or receive non-genuine emails posing as Principals (Steed, 2023).

Furthermore, the insider threat was ever present, as disgruntled students attempted Zoom bombing sending requests to teachers to impose as genuine users to disrupt lessons. The privacy and security settings required greater stringency so external malicious users did not disrupt 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 and evaluate the student's response capabilities. The objective is to increase student efficacy in managing online behaviour, particularly in detecting potential phishing attempts and managing personal data effectively.

The 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 into learning curriculums. The finds of the study could positively influence intervention strategies to improve the teaching curriculums across subject disciplines.

Skeleton of Literature Review

1. INTRODUCTION

a) Background

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.

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)

Research method: Qualitative

Main findings:

Teachers need involvement with administrators.

Teachers are decision-makers on methods of integration for motivation.

Technology training is imperative.

Strengths

Identifies the environment needed.

Limitations

Some views are dated.

Conclusions suggest that more research is needed for best practices

Discrepancies:

Technology has made blended learning possible, but social challenges. Digital staff divide and professional leadership challenges. (Ng et al., 2020)

B. The increase in e-learning adoption by schools

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

Research method: Mixed

Main findings:

Blended learning style.

Online competency issues.

Ad hoc approach to privacy and confidentiality.

Identified lack of digital literacy.

Academic dishonesty.

The COVID-19 pandemic accelerated e-learning in secondary schools.

Strengths

Comprehensive e-learning transition.

Limitations

Focus on Higher Education specifically.

Literature is focused on English-only publications during the pandemic.

C. Cyberawareness of students and practices

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

Research method: Quantitative

Main findings:

Users of the internet are more likely to be cyber aware.

Educational lessons on security would benefit.

Strengths

Awareness scales to measure.

Limitations

401 participants (75.1% female).

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

Research method: Quantitative

Main findings:

Students have a good knowledge of cybersecurity risks, practices and tools.

Students disregard this over time due to usability.

Strengths:

Identified curriculum issues.

Staffing expertise and efficacy

Limitations:

Performed in a live environment, and more safe environment was needed.

Discrepancies:

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).

Research method: Mixed

Main findings:

Perceived good knowledge = Poor performance

Strengths:

Underdeveloped area of research.

Limitations:

Aimed at university-level students.

Discrepancies:

Existing strategies for phishing awareness often overlook simulations. (Irwin, 2023).

E. Implementation of techniques to mitigate phishing attempts

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

Research method: Mixed

Main findings:

Gaining anti-phishing knowledge can increase victimisation as users perceive overconfidence.

Phishing awareness, education, and training should be continued to raise self-efficacy and competence.

Strengths:

Students who protect their information are less likely to be phishing victims.

Limitations:

Limited demographics.

Discrepancies:

Inadequate curriculums (Nicholson et al., 2020)

Research methods

The project will undertake empirical research identifying current approaches to phishing from the literature review and design the simulation accordingly to the findings. The simulation will offer conclusive platforms to collect data in a safe and controlled environment researcher's presence as a qualified and registered educator, surrounded by supportive staff to ease the well-being concerns of participants.

The participants are under the age of 18 years, which adds complexity to the data collected, such as anonymity, privacy and safeguarding vulnerable people. Action research will occur as the participants' inputs directly influence 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) in a mixed method approach gathering quantitative and qualitative data and primary data in assessing their cyber awareness knowledge through multiple choice and open questions in surveys undertaken before and after the simulation. Secondary evidence will be collected 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 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. Interpreting 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 simulation offers participants a safe environment for phishing attempts without real-life consequences. As participants apply their knowledge in this setting, they learn and gain a deeper understanding of managing themselves online, which has a more meaningful impact than reading on the subject.

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 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. The emails will vary in phishing complexity which could include grammatical errors, suspicious URL links, positive or negative information with malicious links and impersonating genuine company emails. The links will not be active in the simulation as the participants will need to view the email and consider reasons for it being genuine or not. 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 interface is aimed to be engaging for the age range and interactive, so this is a memorable and positive learning experience. The nature will be user-friendly, with simple explanations to avoid misunderstandings.

The post-simulation questionnaire will be based on their reflection and cyber awareness since completing the simulation. The aim is to identify any areas they have misunderstandings in when trying to mitigate a phishing attempt and understand the consequences of becoming susceptible to an attack. The artefact will provide participants with the knowledge and improve awareness of tactics by malicious users and the risks from phishing attacks so that when e-learning or online, they are more prepared and equipped to have a safe online presence with good digital literacy and can recognise phishing attempts.

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.

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

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.

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

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].

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. 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.

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].

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].

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*.