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 cyberaware to 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 by utilising 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 of e-learning adoption by schools
C. Cyberawareness 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

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

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

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 need an environment to be decision makers on methods of integration for motivation Committees gain peer support Technology training is imperative
Strengths	Limitations
Identifies the environment needed which is the oppositive of Hong Kong during pandemic years.	Some views are dated Conclusions suggest more research is needed for best practices of technology integration
Discrepancies:	Technology had made blended learning possible in Hong Kong through online classes but barriers to effective teaching and learning. Learners need to socialise with each other, digital divdie with stafd, 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)

Research method:	Mixed
Main findings:	E-learning refers to actual learning that takes place the resources are actually used which goes beyond technology Is a new dynamic for the 21st Century learning
Strengths	Limitations
E-learning is a new wat of learning or improvement on existing education and technology driven	Dated as definitions of e-learning as evolved with technology advancement. Experts involved were mainly higher educational staff
Discrepancies:	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 of e-learning adoption by schools

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

Research method:	Mixed and integrative review
Main findings:	Identification of common technologies used in learning.

	Blended learning style Online competence was an issue. Ad hoc approach to privacy and confidentiality Identified lack of digital literacy in departments Academic dishonesty The COVID-19 pandemic has accelerated the adoption of e-learning in secondary schools (Clark, 2021, Duffin, 2022)
Strengths	Limitations
Comprehensive on e-learning transition. Information from a range of countries including China.	Focus on Higher Education specifically. Literature is focused on English-only publications during the pandemic.
Discrepancies:	

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	Limitations
Awareness scales to measure	401 participants (75.1% female)
Discrepancies:	No relationship between cyberbullying awareness and cyberbullying others.

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. Whilst they implement as initially, they disregard it over time due to usability.
Strengths	Limitations
Methodology supported a positive response from participants. Identified curriculum issues. Staffing expertise and efficacy.	Research was performed in a live environment, and safer environment was needed.
Discrepancies:	WIT program had benefit in supporting students to positive online behaviour and cyberawareness (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:	Students who understood phishing attacks performed worse – overestimation of knowledge.
Strengths	Limitations
Identifies an underdeveloped area of research and requirement for students to learn about phishing with nearly 70% of subjects clicking the phishing link.	Aimed at university level students. Not all participants realised it was an experiment
Discrepancies:	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 impersonation of 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)

Research method:	Mixed
Main findings:	Gaining anti-phishing knowledge can increase victimisation as users perceive over confidence however focus is on instant messaging phishing only. Phishing awareness, education and training should be continued to raise self-efficacy and competence.
Strengths	Limitations
Debate on users who share personal information online. The study suggests those who protect their information are less likely to a phishing victim.	Study not confined to Hong Kong as wide age range of participants in the study (up to 43 years). Cyberawareness focused on age and gender and more demographics could be considered.
Discrepancies:	Current school curriculums inadequately educate students on phishing, leaving them vulnerable to cyber threats (Henshaw,

	2023) (Nicholson et al., 2020) (Belger, 2023). Businesses also face phishing attacks, emphasising the need for educational training.

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.

4. 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.

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.

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].

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].

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). [Accessed 26 March 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., 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.

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.

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.

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.

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*.