1. INTRODUCTION

a) Background

Particularly since the Covid-19 outbreak and in-school face-to-face lesson suspensions, many secondary schools have delivered curriculums via e-learning programs or virtual classrooms such as zoom meetings. In return to face-to-face lessons in subsequent years, many schools have continued to offer lessons using the same technology. For students, this offered a powerful new platform to engage in learning; however, with the rate of implementation, the cybersecurity risks posed a significant threat due to students and staff's limited knowledge and strategies to mitigate potential malicious threats.

Social engineering, particularly phishing, has significantly threatened students, teachers and school stakeholders. This project aims to discuss the threats of Phishing attempts when implementing e-learning in secondary schools with cybersecurity tools/techniques to mitigate risks.

b) Scope

A. E-learning in secondary schools
B. Research gaps
C. Threats and risk management
D. Research method – Mixed: Assess students' cyber awareness and offer training and awareness. Students complete a simulation and make an informed decision on an outcome. Hypothesis – Secondary school students have cyber awareness and can use techniques to mitigate phishing attempts.
E. Phishing simulation artefact
F. Results
G. Discussion of findings

Will not be covered:

- Social engineering methods which do not include phishing
- Other threats to secure architecture, Learning Management Systems, School resources

Title: Cybersecurity tools/techniques in implementing e-learning in secondary schools.

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

Supervisors: **1. Samuel Danso (Confirmed)**
2. TBC

2. BODY

A. E-learning in secondary schools

- Definition of e-learning in secondary schools
- Delivery of teaching e-learning

B. Research Gaps

i) Current gaps in the literature

1 (Lastdrager et al., 2017)
2 (Sağlam et al., 2023)
3 (Zhang-Kennedy & Chiasson, 2021)
4 (Nicholson et al., 2020)

Research method:	
Main findings:	1 Short-term benefits Students often overlooked in the intervention -Supported by (Distler et al., 2021) 2 Variety of strategies for implementing awareness, but no simulation of phishing is mentioned 3 2000-2019 Only six phishing media programs identified 4 Teenagers are poor at detecting phishing and riskier behaviour on unfamiliar messages
Strengths	Limitations
1 Training was through storytelling and age-appropriate 3 Lots of literature studied Offers recommendations for adaptability and usability 4 Lack of phishing education in curriculums. Need from teachers.	1 Primary students Paper-based test 3 Not aimed at secondary students
Discrepancies:	

C. Threats and Risk

- Insider threats
  Malicious students
  Disgruntled staff or stakeholders

- External threats
  Malicious outsiders
- Social engineering method: Phishing
- Risks posed / STRIDE

D. Research method

Research method – Mixed
Assess students' cyber awareness and offer training and awareness.
-Questionnaire/Survey

Students complete a simulation and make an informed decision on an outcome.
-Artefact

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

Following educational awareness and simulation, the aim is for students to gain an improved understanding and can mitigate phishing attempts.

E. Artefact

To produce a social engineering simulation aimed at students in support of mitigating various phishing attempts.

This could be part of an introductory programme for students attending e-learning courses or online lessons.
Simulations have been designed at the adult level for professionals, with limited research produced for secondary school students and inclusion in curriculum design.

Simulation is aimed to be hosted in a secure web application whereby students can set up a login account. The web application will have a serious of challenges or scenarios which are pitched at the student level. There will be admin and client modules with security considerations in place.

The aim is to appropriately challenge and engage students, motivating them to practice cybersecurity techniques in real-life settings. The research will try to design scenarios around trending applications that students commonly use or are familiar with.

Using Python due to the libraries available and coding experience.
The simulation will hope to provide data for analysis to determine students' cybersecurity knowledge and responses to given scenarios.

F. Results

G. Discussion of findings

F. Results

3. CONCLUSION

Summary of findings
Justification for the project
Significant findings
Future priorities and research gaps

4. REFERENCES

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.

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

Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. & Anderson, P. (2020). *Investigating Teenagers' Ability to Detect Phishing Messages*.

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.

Zhang-Kennedy, L. & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.,* 54, (1): Article 12.