Unit 2 Project Proposal Outline – Jonathan Callaghan

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

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

Proposed research problem:

- Technology integration in school curriculums has made it challenging to define e-learning conclusively (Sangrà et al., 2012).
- E-learning should encompass electronic, mobile, and digital learning to enhance students' learning experience (Rodrigues et al., 2019) (Basak et al., 2018).
- The COVID-19 pandemic has accelerated the adoption of e-learning in secondary schools (Clark, 2021) (Duffin, 2022).
- Phishing is a prevalent form of social engineering that disrupts e-learning (Lastdrager, 2014) (Diaz et al., 2020).
- Existing strategies for phishing awareness often overlook simulations, which could be valuable for secondary school students (Irwin, 2023) (Sağlam et al., 2023).
- Current school curriculums inadequately educate students on phishing, leaving them vulnerable to cyber threats (Henshaw, 2023) (Nicholson et al., 2020) (Belger, 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).
- Businesses also face phishing attacks, emphasising the need for educational training.

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

Proposed aims and objectives:

- Using the STRIDE methodology, identify threats and assess the risk posed by phishing attacks.
- Design and evaluate a simulation-based educational intervention for secondary school students to enhance phishing awareness and response capabilities.

Proposed research design:

- A mixed-method approach to gain quantitative and qualitative data.
- Gantt chart to manage deadlines, milestones and progress.
- Primary evidence: Surveys/Questionnaire/Results (Training/Artefact).

  Secondary evidence: Literature reviews, Statistical reports.

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

Artefact(s) that can be created:

- Design a web-based application on social engineering simulation for students to mitigate phishing attempts—Python programming language with Flask.
- Secure web application with login accounts, admin and client modules, and security considerations.
- Challenges/scenarios pitched at the student level to engage and motivate cybersecurity practice around trending applications familiar to students.
- Data analysis to assess students' cybersecurity knowledge and responses

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.

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].

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.

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].

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

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.