A Social Engineering Ontology and Knowledge Graph for Risk Management.

Akintokun Omowumi & Dr. Christopher Mcdermott

Aims & Objectives

The aim of this paper is to enhance the risk assessment process of an organisation by providing useful insights on the risk and impact of social engineering attacks in the overall risk quantification to enable proper classification and prioritization of the identified risk.

The objective of the paper is to develop a knowledge graph for the social engineering attacks and accessing its impact. The specific objectives of this research are as follows:

- Critically analyse existing literatures on social engineering attack.
- Review existing standard and framework for cybersecurity assessment including NIST cybersecurity framework, NCSC Cybersecurity Assessment Framework, COBIT 2019, and ISO 27001-2022.
- Provide social engineering ontology and knowledge graph.
- Consider the human weaknesses targeted in the social engineering attacks.
- Consider Legal, ethical, social and professional implication of knowledge graph and simulated phishing email.
- Evaluate the effectiveness and user satisfaction of the solution and seek improvement opportunities for future research.

Methods

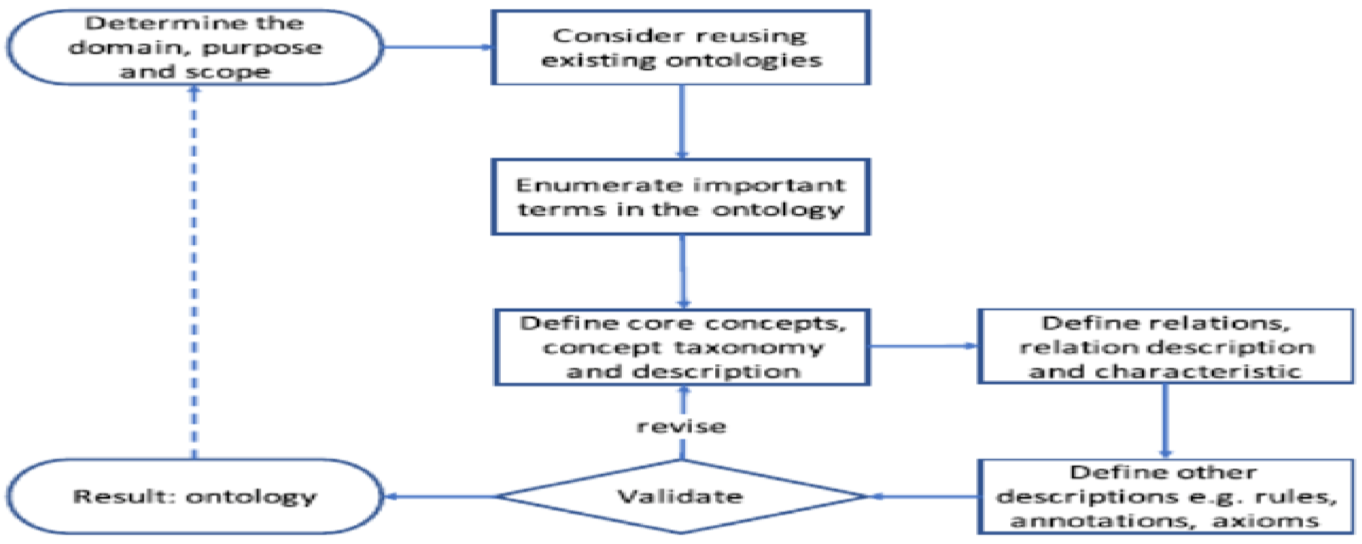
Determine the domain, purpose and scope
Consider reusing existing ontologies
Enumerate important terms in the ontology
Define core concepts, concept taxonomy and description
Define relations, relation description and characteristic
revise
Result: ontology
Validate
Define other descriptions e.g. rules, annotations, axioms

Figure 1: Overview of methodology to develop domain ontology of social engineering (Wang et al. 2021)

The paper adopted a phased approach that includes requirements documentation, development of use cases, design and development, testing, implementation, and evaluation. The process started with clearly defined requirements based on interactions with end users and literature review, and different use cases for the knowledge graph were documented and reviewed.

The design commenced from the existing ontology using protege to demonstrate the different concepts that form the body of social engineering and clearly depicts the relationships and interaction between the entities. To take advantage of the advanced functionalities in the Neo4j, the ontology was exported from protege and imported into Neo4j database which them become the knowledge base. Using the simulated phishing data to build the knowledge and querying it using the Cypher –Neo4j descriptive query language. Evaluation of the possible scenarios to determine its accuracy and relevance. Lastly, risk quantification was done taking into consideration the insights from the knowledge graph.

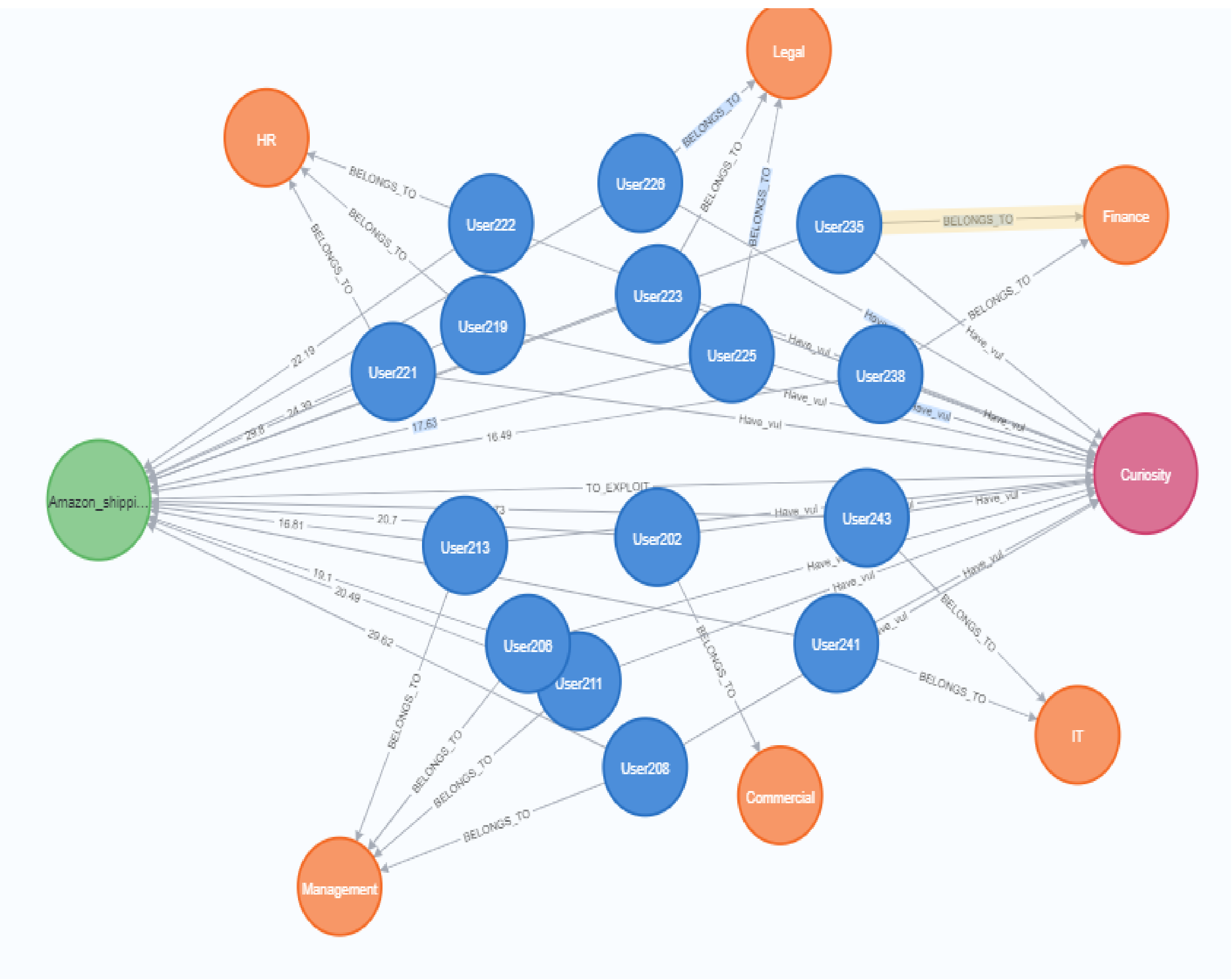

Figure 2: Overview of users' response within 30 seconds

Conclusions

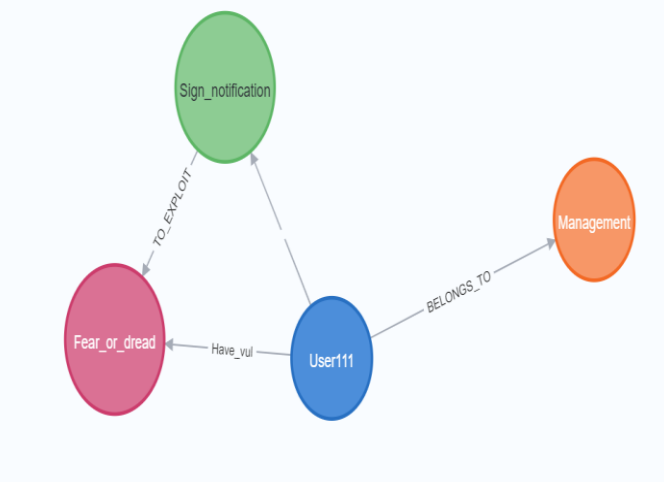

Figure 3: Overview of users who reported the phishing)

This paper leverages anonymized simulated phishing data to analyse and understand how users would respond to tactics used by threat actors. Integration of this data into an ontology and knowledge graph provides insights on the structures and connects information on social engineering strategies.

The result indicates people are more susceptible to simulated phishing that targets "Curiosity". Evidenced by users clicking within 30 seconds of receiving the email. Only one user reported the email as phishing. This risk is quantified based on its likelihood and impact on the organization. For this study, cipher provides the interface for querying the knowledge, future work will explore the use of Large Language Models (LLM) to enhance user experience.

Acknowledgments

I would like to express my profound gratitude to Dr. Chris McDermott, whose expertise, support, and guidance played a huge part in the successful completion of this project. The insightful feedback and constructive criticism have been crucial throughout every phase of the project. My sincere appreciation goes to Robert Gordon University (RGU) for providing an enabling environment and resources to carry out this work.

RGU SCHOOL OF COMPUTING

MSc Project – Cyber Security.