

Kantu Bill

Kantu Bill and group

 BBC III Proposals Submission November 23 2025

 BBC IT Project Reports

 Makerere University Business School

Document Details

Submission ID**trn:oid::1:3421584229****Submission Date****Nov 23, 2025, 3:12 PM GMT+3****Download Date****Nov 23, 2025, 8:51 PM GMT+3****File Name****PROJECT_PROPOSAL_Signed.pdf****File Size****760.0 KB****22 Pages****3,687 Words****25,345 Characters**



75% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

-  **47 AI-generated only 75%**
Likely AI-generated text from a large-language model.
-  **0 AI-generated text that was AI-paraphrased 0%**
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.



MAKERERE UNIVERSITY BUSINESS SCHOOL

Development of an AI- Powered cybersecurity Awareness Chatbot for Education Users on Online Threats and Best Practices

By

Name	Registration Number	Phone Number
KIZITO ABDURAHIM	23/U/10168/PS	0704225091
NANTUMBWE GEORGIA	23/U/15329/PS	0743180602
KALIZA AFUSWA	23/U/00492/EVE	
KANTU BILL	23/U/08990/PS	0762387854
ASIIMWE BUNNET	23/U/06672/EVE	0709900695

Supervised by

Dr. Abdal Kasule (PhD)

Department of Information Systems

**A Project Proposal Submitted to the Faculty of Computing & Informatics of Makerere
University Business School in Partial Fulfillment for the Award of the BBC
of Makerere University**

November, 2025

DECLARATION

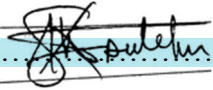
We, the undersigned, declare that to the best of our knowledge, this proposal is our original piece of work, and has never been published and submitted for any award in any other University or Higher Institution of Learning.

Name	Registration Number	Signature
KIZITO ABDURAHIM	23/U/10168/PS	
NANTUMBWE GEORGIA	23/U/15329/PS	
KALIZA AFUSWA	23/U/00492/EVE	
KANTU BILL	23/U/08990/PS	
ASIIMWE BUNNET	23/U/06672/EVE	

Date:

APPROVAL

This project proposal has been submitted with my approval as supervisor and my signature is here appended:

Signed..........

Date: ...22nd November 2025

Name...Dr. Abdal Kasule (PhD.).....

Makerere University Business School

Table of Contents

DECLARATION	ii
APPROVAL	iii
Table of Contents.....	iv
LIST OF ABBREVIATIONS.....	1
1.0 INTRODUCTION.....	2
1.1 Background to the Study.....	2
1.2 Statement of the Problem	3
1.3 Project Goal and Objectives.....	4
1.4 Specific Objectives of the Study.....	4
1.5 Study Scope	4
1.5.1 Subject/ Conceptual Scope	4
1.5.2 Geographical Scope	4
1.5.3 Time Scope.....	4
1.6 Significance of the Study	5
LITERATURE REVIEW.....	6
2.0 Introduction.....	6
2.1 Cybersecurity Awareness and Human Vulnerability	6
2.2 Chatbots in Education and Awareness	6
2.3 AI, NLP, and Machine Learning in Chatbots	6
2.4 Existing Cybersecurity Chatbots and Related Works	7
RESEARCH METHODS	8
3.0 Introduction.....	8
3.1 Research Design/ Research Approach.....	8
Illustration of DSR Process:.....	8
Key Components of the DSR Approach:.....	9
3.2 Study Population	10
3.3 Sampling Technique	10
3.4 Sources of Data.....	10
3.5 Requirement Elicitation [Data Collection] Techniques.....	11
3.6 System Analysis And Design	11
3.7 System Design Approach	11
3.8 Limitations Of The Project	12
3.9 Ethical Considerations	12
4.0 TIMELINE.....	13

4.1 PROPOSED BUDGET	14
References	15

LIST OF ABBREVIATIONS

AI: Artificial Intelligence

API: Application Programming Interface

BBC: Bachelor of Business Computing

DSR: Design Science Research

ML: Machine Learning

NLP: Natural Language Processing

SDLC: Systems Development Life Cycle

UBA: User Behavioral Analytics

1.0 INTRODUCTION

In the digital age, cybersecurity threats are evolving at an alarming rate, posing significant risks to individuals, businesses, and governments worldwide. Cyberattacks such as phishing, malware, ransomware, and social engineering have become more sophisticated, leading to financial losses, data breaches, and reputational damage. The rapid expansion of digital technologies has led to an increase in cybersecurity threats worldwide. The AI-powered Cybersecurity Awareness chatbot will leverage Natural Language Processing (NLP) and Machine Learning (ML) techniques to provide personalized cybersecurity advice based on user interactions. By simulating real-world cyber threats, such as phishing attempts and password security scenarios, the chatbot will enhance user engagement and retention of critical cybersecurity knowledge.

1.1 Background to the Study

According to cyber security reports, human error remains one of the leading causes of security incidents, in accordance to Infosec magazine staff (2020) 'Human Error: The leading cause of Cybersecurity Breaches', the article emphasizes the prevalence of human error in security breaches. Despite the availability of cybersecurity training programs, traditional learning methods such as reading lengthy articles, attending webinars, or completing online courses often fail to engage users effectively. Based on Van der Meijden (2020) 'Cybersecurity Training: The Importance of Engagement', the article discusses the shortcomings of traditional training methods. Many individuals either lack the technical knowledge or the patience to go through these resources leaving them vulnerable to cyber threats. Following Furnell (2020) 'Cyber Security: The Role of Users', he discusses the critical role of users play in cybersecurity and the consequences of their lack of technical knowledge. One of the major cybersecurity breaches that have happened in Uganda was the 16.8 million dollars that was swindled from bank of Uganda in 2021 as published in New Vision by Kasozi (2021), 'Cybersecurity Breach at Bank of Uganda:\$16.8 million stolen'. In another cybersecurity incident, NIRA, a national identification and registration authority was involved in a sex trafficking scandal where it was giving out personal information to unauthorized users as sighted by Ochieng (2022), 'BBC Investigation Exposes NIRA's role in Trafficking Network' in Daily Monitor. Furthermore, another incident occurred in 2020 where there was a data breach at harrods that involved a third party provider and reassured customers that sensitive payment information wasn't affected as

sighted by Smith(2020) ‘Harrods Data Breach: Customer Information Exposed’.

With cybercrime becoming an ever-growing global concern, fostering cybersecurity awareness is more crucial than ever. This project aims to empower users with the knowledge and skills needed to navigate the digital world safely. By bridging the gap between cybersecurity education and user engagement, the proposed chatbot will serve as a valuable tool in promoting online safety and reducing human-related security risks.

1.2 Statement of the Problem

The purpose for developing this AI powered cybersecurity chatbot is to raise awareness among end users in such a way that it educates users about cybersecurity threats, best practices and how to recognize phishing attempts or malware. Also, to assist in identifying suspicious activities or potential breaches in real time. The chatbot is to also provide step by step instructions on how to respond to cybersecurity incidences such as data breaches or ransomware attacks. With all the above that has been discussed there is still a large number of individuals that are still unaware or simply illiterate about cybersecurity threats because of a number of reasons such as; cybersecurity terminology can be complex and intimidating making it difficult for a number of people to understand. Symantec (2019) ‘The Complexity of Cybersecurity: Understanding the Threat Landscape’. There is also a lot of misinformation available online which leads to confusion and difficulty in discerning credible sources which misleads a number of end users who in turn become uncertain on what to believe in. Pew Research Center (2020)’ The Challenges of Information Overload in Cybersecurity’. The major factor for cybersecurity illiteracy is overconfidence. Many end users are sure that cyber threats do not affect them personally leading to complacency. Cybersecurity and infrastructure security Agency (2021) ‘Understanding the Cybersecurity Complacency’. Cybersecurity illiteracy has a number of negative effects to end users like, unaware individuals can fall victim to phishing scams and providing sensitive information to attackers. lack of knowledge can also lead to malware infections and compromising personal data. There is also financial theft. Cyber criminals can access bank accounts or credit card information leading to financial losses. Cybersecurity Ventures (2020) ‘Cybercrime to Cost the World \$10.5 Trillion Annually by 2025’. There is also reputation damage where organisations affected by cyber incidents often receive a bad public image and

negative media attention which can erode customer trust. Harris (2020) 'The Impact of Cyber Attacks on Brand reputation'.

1.3 Project Goal and Objectives.

The purpose of this project was to design and develop an AI-powered Cybersecurity Awareness Chatbot to educate users on online threats and best practices in an interactive and engaging manner.

1.4 Specific Objectives of the Study

- i. To identify common cybersecurity threats and user vulnerabilities by analyzing recent cybersecurity reports and attack trends.
- ii. To design an AI-driven chatbot that educates users on cybersecurity best practices through real-time interactions.
- iii. To develop an AI-driven chatbot that educates users on cybersecurity best practices through real-time interactions.
- iv. To implement Natural Language Processing (NLP) and Machine Learning (ML) in the chatbot to enhance its ability to understand and respond to user queries.

1.5 Study Scope

1.5.1 Subject/ Conceptual Scope

This project was confined to the development of a chatbot for cybersecurity awareness. Its knowledge base covered common threats like phishing, malware, and social engineering, and best practices such as password hygiene and email safety.

1.5.2 Geographical Scope

The study was conducted within the Makerere University academic community, though the developed chatbot was designed to be accessible online to a wider Ugandan audience.

1.5.3 Time Scope

The project was executed over a period of eight months, from February 2025 to December 2025.

1.6 Significance of the Study

- a) **Significance to the community:** The chatbot provides an easily accessible tool for students and the public to improve their cybersecurity knowledge, potentially reducing their victimization by online scams.
- b) **Significance to the industry:** The project demonstrates a practical application of AI and chatbot technology for educational purposes, which can be adopted and scaled by organizations for staff training.
- c) **Significance to other researchers:** It contributes to the academic body of knowledge on using conversational AI for security awareness and provides a foundation for further research in this domain.
- d) **Significance to the Students:** The project provided the development team with hands-on experience in AI, NLP, software development, and project management, aligning with the practical skills required for the Bachelor of Business Computing degree.

LITERATURE REVIEW

2.0 Introduction

Literature Reviews refers to existing literature related to the key concepts of this project. It covers cybersecurity awareness, the role of chatbots in education, the underlying AI technologies, existing cybersecurity chatbot implementations, and identifies the gaps that this research aimed to fill.

2.1 Cybersecurity Awareness and Human Vulnerability

Arora et al. (2023) report that human vulnerability remains the weakest link in the cybersecurity chain, with studies consistently showing that over 90% of security breaches originate from human errors such as clicking malicious links or using weak passwords. Fung and Lee (2022) emphasize that despite the known risks, many internet users are still unaware of the cyber threats surrounding them. In Uganda, the National Information Technology Authority (NITA, 2021) found that over 60% of internet users could not identify a phishing email, highlighting a critical awareness gap at the national level.

2.2 Chatbots in Education and Awareness

Lee et al. (2020) demonstrated that chatbots, or conversational agents, have emerged as powerful tools in education and customer service due to their 24/7 availability, scalability, and interactive nature. In the educational domain, their study showed the effectiveness of a chatbot for instantly answering students' questions in a university course. Similarly, Clarizia et al. (2020) developed a chatbot to support students in learning cultural heritage. These studies indicate that chatbots can provide personalized, on-demand learning experiences, offering a significant advantage over static training materials.

2.3 AI, NLP, and Machine Learning in Chatbots

Adamopoulou and Moussiades (2020) explain that the core intelligence of modern chatbots is driven by Artificial Intelligence (AI), particularly Natural Language Processing (NLP) and Machine Learning (ML). NLP enables chatbots to understand and interpret human language,

while ML allows them to learn from interactions and improve their responses over time. Platforms such as Google Dialog flow and IBM Watson provide robust frameworks for developing these intelligent agents. Fung and Lee (2022) successfully utilized Google Dialog flow to create a cybersecurity expert chatbot, demonstrating the practicality of such platforms for building domain-specific conversational interfaces.

2.4 Existing Cybersecurity Chatbots and Related Works

Several chatbots have been developed for cybersecurity purposes. Microsoft has introduced Security Copilot, while IBM developed Watson for Cybersecurity, both of which are advanced systems designed to assist security professionals. In the academic sphere, Fung and Lee (2022) developed a chatbot for promoting cybersecurity awareness, which provided term definitions, self-quizzes, and a workflow for identifying phishing emails. Similarly, Arora et al. (2023) created a chatbot deployed on Twitter to perform sentiment analysis on tweets for assessing cybersecurity threats, demonstrating the potential of chatbots in threat intelligence gathering.

RESEARCH METHODS

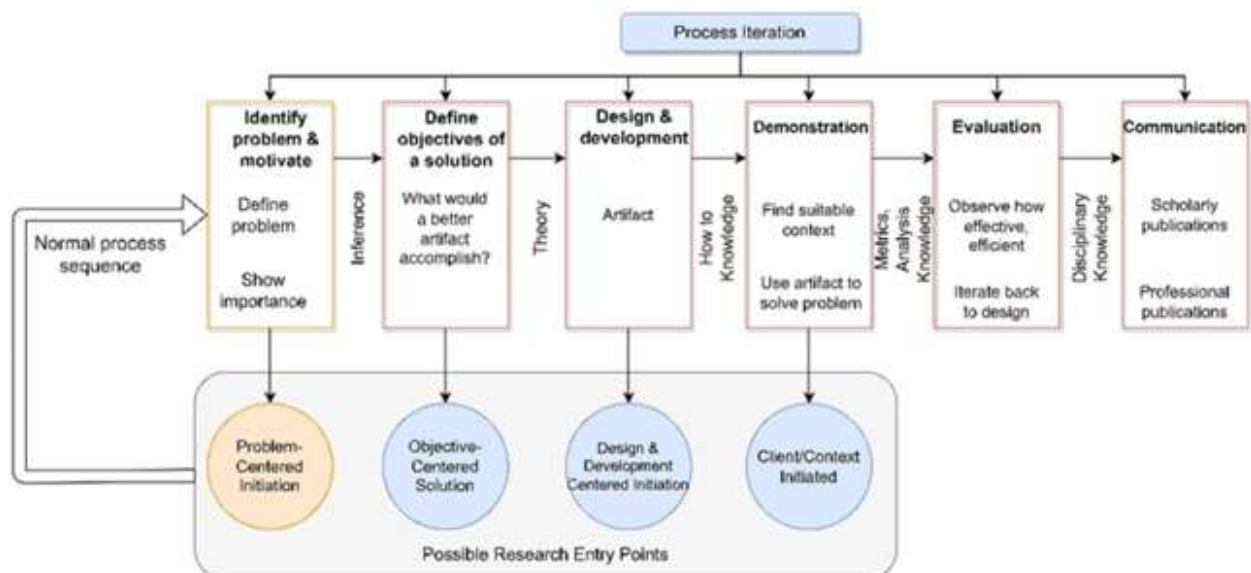
3.0 Introduction

This chapter outlines the research methods that guided the development of the AI-powered Cybersecurity Awareness Chatbot. It details the chosen research design, the study population and sampling techniques, sources of data, requirements elicitation methods, the system analysis and design approach, and the project's limitations and ethical considerations.

3.1 Research Design/ Research Approach

Peppers et al. (2007) propose the Design Science Research (DSR) approach as particularly well-suited for projects that aim to create innovative IT artifacts. In this project, the DSR methodology was adopted to develop an AI-powered chatbot designed to address a recognized organizational problem. The DSR process was executed through the following phases:

Illustration of DSR Process:



Development of an AI powered cybersecurity chatbot using design science research method

Key Components of the DSR Approach:

- **Problem Identification:** The project starts with an in-depth investigation into contemporary cybersecurity challenges. This includes understanding how common cyberattacks such as phishing, malware, ransomware, and social engineering pose risks to users at all levels. Data will be gathered through interviews, focus groups, and surveys with individual users, cybersecurity experts, and IT professionals, emphasizing issues like human error and the limitations of traditional training methods. *Example:* Combining online questionnaires with in-person interviews to uncover why conventional cybersecurity training fails to engage users effectively.
- 1. **Objective Definition.** Clear project objectives will be defined based on initial problem identification. These objectives include analyzing existing cybersecurity education shortcomings, designing a user-centered conversational interface, and developing dynamic response capabilities that mimic real-world cyber threat scenarios. The overarching goal is to enhance user engagement and retention of essential cybersecurity knowledge.
- **Design & Development of the conceptual model:** This phase involves creating a conceptual model for the cybersecurity chatbot, followed by developing a working prototype. Key functionalities such as contextual threat detection, personalized security guidance, and interactive simulation of cyber-attack scenarios will be incorporated into the system. *Reference Concept:* Drawing from established design science literature (e.g., Peffers et al., 2007; Hevner et al., 2004), iterative development will be employed to ensure the solution aligns with real-world cybersecurity training needs.
- 2. **Evaluation:** The chatbot prototype will undergo thorough evaluation through usability testing, performance metrics, and security assessments. A pilot deployment will be carried out involving diverse user groups to determine if the system effectively improves cybersecurity awareness and reduces vulnerabilities related to human error. *Example:* A phased rollout with controlled user groups, followed by surveys and performance testing, will measure the chatbot's impact on user behavior and knowledge retention
- **Communication:** The final phase involves documenting the entire development process, the evaluation results, and the lessons learned. Findings will be shared with academic communities

as well as industry stakeholders to contribute to the broader discourse on cybersecurity education.

An adapted illustration of the DSR process based on foundational research such as that by Peffers et al. (2007) and Hevner et al. (2004) will be utilized to demonstrate the progression from problem identification to evaluation and dissemination. Each stage is meticulously designed to support the established objectives of creating an engaging and effective cybersecurity awareness tool.

3.2 Study Population

The project focused on two primary stakeholder groups:

- **End-Users:** Students and young adults within the Makerere University community, who are active internet users but may have varying levels of cybersecurity knowledge.
- **IT Administrators and Cybersecurity Professionals:** IT administrators from the public and private sectors, including cybersecurity consultants and IT department staff. Their insights will be invaluable for aligning the chatbot's functionalities with real-world threat scenarios and validating its technical robustness.

3.3 Sampling Technique

A combination of sampling techniques was employed:

- **Purposive Sampling:** This was used to select IT professionals and cybersecurity experts. These individuals were chosen specifically for their expertise to ensure the technical robustness and accuracy of the chatbot's knowledge base.
- **Convenience Sampling:** This was used to select end-users (students) for the preliminary evaluation. Participants were selected based on their availability and willingness to participate.

3.4 Sources of Data

The project utilized both primary and secondary data:

- **Primary Data:** This was collected through direct interaction with the chatbot during testing and from feedback forms used in the pilot evaluation. This data helped assess the user

experience and the chatbot's performance.

- **Secondary Data:** This was extensively used and included academic journals, conference papers (such as Fung & Lee, 2022; Arora et al., 2023), cybersecurity reports from organizations like NITA-U, and online resources for building the chatbot's knowledge base.

3.5 Requirement Elicitation [Data Collection] Techniques

To gather the necessary information for designing the system, the following requirement elicitation techniques were used:

- **Surveys and Questionnaires:** Distributed among potential end users to collect insights on cybersecurity knowledge, digital literacy levels, and preferred learning methods.
- **Interviews:** Conducted with IT professionals to gather detailed inputs on current best practices and the practical aspects of cybersecurity education.
- **Observation:** The team observed users interacting with existing cybersecurity training materials and other educational chatbots to understand common usability pitfalls and desirable interaction patterns.

3.6 System Analysis And Design

A Structured Systems Analysis and Design approach was adopted. This involved breaking down the system into smaller, manageable components and defining the data flows between them. The focus was on the logical structure of the system, ensuring that each module (e.g., user interface, NLP engine, knowledge base) functioned cohesively to meet the overall objectives.

3.7 System Design Approach

The Agile methodology was used for the system development. This iterative approach allowed for the creation of the chatbot in cycles or "sprints." Each sprint resulted in a working increment of the system, which was then reviewed and improved upon in the next sprint. This approach was chosen because it allowed for flexibility in incorporating feedback and adapting to challenges encountered during development, such as fine-tuning the Dialogflow intents or modifying the quiz logic.

3.8 Limitations of the Project

Several constraints were encountered during the project:

- a) **Technical Limitations:** The project relied on the Google Dialogflow platform, which, while powerful, has usage quotas on its free tier that could limit scalability. Furthermore, the chatbot's knowledge base was manually curated and may not cover every possible cybersecurity term or emerging threat.
- b) **Resource Limitations:** The project was developed with limited financial resources, restricting access to premium APIs or advanced AI models. Development was constrained to open-source technologies and free-tier cloud services.
- c) **Time Constraints:** The project timeline was limited to one academic semester, which affected the depth of testing and the number of features that could be implemented. A more extensive pilot study with a larger user base could not be conducted.
- d) **Scope Limitations:** The chatbot was designed as a web application and was not integrated into popular messaging platforms like WhatsApp or Telegram during this phase, which could have increased its accessibility.

3.9 Ethical Considerations

Ethical integrity was maintained throughout the project:

- **Data Privacy:** During the pilot evaluation, any data collected from users was anonymized. The chatbot was designed not to store personally identifiable information from conversations.
- **Informed Consent:** Participants in the evaluation phase were informed about the purpose of the study and how their feedback would be used. Their participation was voluntary.
- **Academic Integrity:** All sources of information, including code snippets and literature, have been properly cited to avoid plagiarism.

Appendix 1: TIMELINE

PHASE	DURATION
Requirement gathering	6 weeks
System design	8 weeks
Prototype development	10 weeks
Testing and evaluation	4 weeks
Documentation	4 weeks
Total project duration	32 weeks

Appendix 2: PROPOSED BUDGET

Category	Amount
Personnel	
Project manager	1,500,000
AI/NLP developer	2,000,000
UX/ UI designer	2,500,000
Cybersecurity consultant	1,500,000
Software and tools	
NLP/ML frameworks	500,000
Chatbot platform	500,000
Development tools	2000,000
Hardware	
Laptops	700,000
Servers/cloud infrastructure	400,000
User testing	
Participant incentives	2000,000
Usability lab rental	2,500,000
Miscellaneous	
Communication	1,500,000
Contingency	1000,000
Total budget	17,100,000

References

Adamopoulou, E., & Moussiades, L. (2020). An overview of chatbot technology. In *IFIP International Conference on Artificial Intelligence Applications and Innovations* (pp. 373-383). Springer, Cham.

Arora, A., Arora, A., & McIntyre, J. (2023). Developing Chatbots for Cyber Security: Assessing Threats through Sentiment Analysis on Social Media. *Sustainability*, 15(17), 13178.

Clarizia, F., Colace, F., Lombardi, M., & Santaniello, D. (2020). A chatbot for supporting users in cultural heritage contexts.

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Understanding cybersecurity complacency*. U.S. Department of Homeland Security.

Cybersecurity Ventures. (2020). *Cybercrime to cost the world \$10.5 trillion annually by 2025*. Cybersecurity Ventures Annual Report.

Fung, Y. C., & Lee, L. K. (2022). A Chatbot for Promoting Cybersecurity Awareness. In *Cyber Security, Privacy and Networking* (pp. 379-387). Springer, Singapore.

Furnell, S. (2020). *Cyber security: The role of users*. Journal of Cybersecurity Education, Research and Practice.

Harris, J. (2020). *The impact of cyber attacks on brand reputation*. Brand Protection Journal.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). *Design science in information systems research*. MIS Quarterly, 28(1), 75–105.

Infosec Magazine Staff. (2020). *Human error: The leading cause of cybersecurity breaches*. Infosec Magazine.

Kasozi, A. (2021). *Cybersecurity breach at Bank of Uganda: \$16.8 million stolen*. New Vision.

Lee, L. K., Fung, Y. C., Pun, Y. W., Wong, K., & Yu, W. (2020, November). Using a multiplatform chatbot as an online tutor in a university course. In *2020 International Symposium on Educational Technology (ISET)* (pp. 53-56). IEEE.

National Information Technology Authority - Uganda (NITA-U). (2021). *National Cybersecurity*

Report.

Ochieng, L. (2022). *BBC investigation exposes NIRA's role in trafficking network*. Daily Monitor.

Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Pew Research Center. (2020). *The challenges of information overload in cybersecurity*. Pew Research Center.

Smith, J. (2020). *Harrods data breach: Customer information exposed*. Cybersecurity News Report.

Symantec. (2019). *The complexity of cybersecurity: Understanding the threat landscape*. Symantec Security Report.

Van der Meijden, A. (2020). *Cybersecurity training: The importance of engagement*. Cybersecurity Journal.