Enhancing AI Healthcare Security Through Public Education: Innovative Awareness Platform Design

KIANA BEPETE
s5405921@bournemouth.ac.uk
CYBER SECURITY MANAGEMENT
DEPARTMENT OF SCIENCE AND TECHNOLOGY
BOURNEMOUTH UNIVERSITY

INTRODUCTION

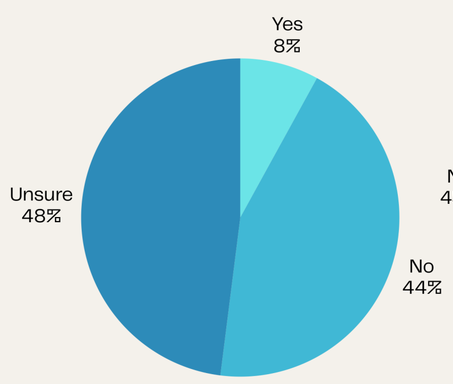
Generative artificial intelligence (AI) has rapidly become ubiquitous across various industries, including healthcare, finance, and media, catalyzed by events like the COVID-19 pandemic. Its applications in healthcare, from research and diagnostics to patient care, are expected to drive the AI in healthcare market to $173.55 billion by 2029. Despite its benefits for both technical and non-technical users, there is a lack of awareness regarding cybersecurity risks associated with generative AI, particularly in healthcare.

Educating the public about these risks is crucial to promoting responsible use and reducing dependency on AI. This research focuses on a specific user who are vulnerable to social engineering and cyber psychological manipulation due to the health implications involved. Addressing this gap in cybersecurity awareness is essential to ensure the safe and ethical utilization of generative AI in healthcare and other sectors.

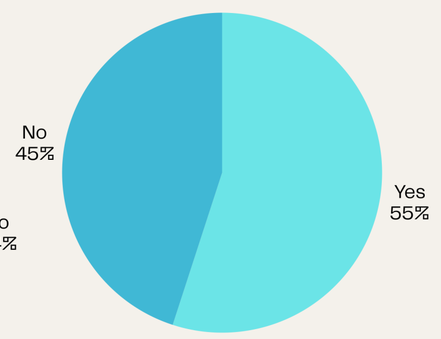
METHODOLOGY

A mixed method approach is employed in this dissertation, which combines both primary and secondary data collection methods in order to investigate proactive cybersecurity education. Through iterative cycles of planning, action, observation, and reflection, the educational platform will continuously be improved. Primary data was gathered through questionnaires to measure AI users' behaviours and awareness and perception of cyber security. Secondary data included literature reviews to formulate the problem environment and inform platform design and content. Qualitative analysis techniques, such as open-ended responses, were employed alongside quantitative analysis of survey data using statistical tools.

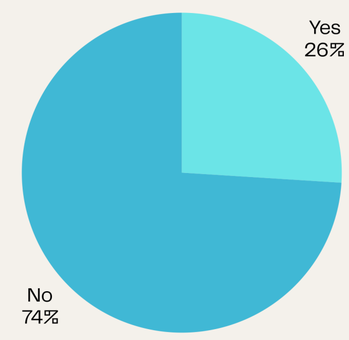
RESULTS



SUFFICIENT CYBER SECURITY MEASURES ARE IN PLACE IN CHAT GPT



AWARE OF THE CYBERSECURITY RISKS ASSOCIATED WITH THE USE OF AI FOR HEALTHCARE



CONSIDERED QUERING FOR HEALTH ADVISE, HEALTH SOLUTIONS OR DIAGNOSIS

ANALYSIS

- 71% of users of Generative AI, such as CHatGPT, seek medical advice, health solutions, or diagnosis.
- One third of the 15% of individuals who had used generative AI for health care had shared personal information with others.
- According to only 8% of users, AI systems are adequately protected by cyber security measures.
- 12% of users would recommend non-users to use generative AI for health solutions, health advice or diagnosis
- 55% of individuals are unaware of cybersecurity risks associated with AI use for healthcare
- Only 1% of respondents are 'extremely confident' that the information provided is accurate. 14% are 'somewhat confident'.
- 17% of responders are 'Extremely not confident' in their awareness of social engineering and 19% are 'Somewhat not confident'

CONCLUSION

In view of the increasing use of AI systems, specifically for the purposes noted above, it is imperative that users are educated on the risks and threats associated with the use of their information and data. Research has shown that more than half of users are unaware of potential hazards, therefore, targeting this element would be an effective mitigation strategy when dealing with the increasing rate of cyber attacks on artificial intelligence and the manipulation of health-related assets.