KABARAK UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE & IT

RESEARCH PROPOSAL

Title: Social Engineering: An Examination of Techniques, Impacts, and Mitigation Strategies

A Project Proposal Submitted in Partial Fulfillment of the Requirements for the Award of Bachelor of Science in Computer Security and Forensic Degree of Kabarak University

Rumeisa Mwanamisi – BSCSF/MK/2995/09/24

March 2025

Abstract

Social engineering has become a great risk of cybersecurity, using psychological tactics to take advantage of human errors instead of technical flaws. This research proposal aims to create a specific framework to combat threats to social engineering at the University of Kabarak. Research plans to discover widespread social technical methods such as fraud, requirements and bait, assessing their effects and developing effective impaired strategies suitable for university. Using a mixed method strategy, research will integrate quantitative surveys, qualitative interviews and simulation attack scenarios to assess users' awareness and recovery ability of the system. The results will help improve network security strategies by combining cognitive training, technical measures and incident response processes. Finally, this initiative aims to reduce the dangers related to social technical attacks while promoting awareness of cybersecurity in the entire university community

Table of Contents

Abstract ..... **i**

Chapter 1: Introduction **1**

1.1 Introduction **1**

1.2 Background of the Study **1**

1.3 Problem Statement **1**

1.4 Objectives **2**

1.4.1 Main Objective 2

1.4.2 Specific Objectives 2

1.5 Research Questions **3**

1.6 Significance of the Study **3**

1.7 Scope and Limitations of the Study **4**

1.8 The limitations of this study **4**

1.8 Proposed Modules **4**

Chapter 2: Literature Reviews **6**

2.1 Introduction **6**

2.2 Social Engineering Techniques **6**

2.2.1 Phishing 6

2.2.2 Pretexting 6

2.2.3 Baiting 6

2.2.4 Quid pro 7

2.2.5 Tailgating 7

2.3 Impact of Social Engineering Attacks **7**

2.3.1 Data Breaches 7

2.3.2 Financial loss 7

2.3.3 Reputation damage 7

2.4 Mitigation strategy **7**

2.4.1 Cognitive raising training 7

2.4.2 Technical Control 8
2.4.3 Reactions from incidents 8
2.5 Gaps in the Literature 8
2.6 CONCLUSION 8
Chapter 3: Research Methodology 9
3.1 Introduction 9
3.2 Research design 9
3.3 Data Collection Methods 9
3.4 Sample Population 11
3.4.1 Sampling Strategy: 11
3.4.2 Sample Size Determination: 11
3.5 Data Analysis Techniques 12
Quantitative Analysis: 12
Qualitative Analysis: 12
Mixed-Methods Integration: 13
3.6 Research Ethics 13
3.7 Conclusion 14
References **15**

Chapter 1: Introduction

1.1 Introduction

This chapter provides the basic things of the research project, focusing on social engineering as an important threat of cyber security. Social engineering, controlling individuals revealing secret information or performing harmful actions for themselves or for their organization, has become a vector of a sophisticated and comprehensive attack. This study is aimed at intensive inspection of techniques used by social engineers, to assess the impact of successful attacks and offer effective strategies for organizations and individuals. The project includes an analysis of psychological principles exploited by social engineers, recent trends in attacking methods and developing a framework to improve awareness and recovery of social techniques.

1.2 Background of the Study

Social technical attacks have increased significantly in recent years, exploiting human factors in security systems. Traditional security measures, such as firewalls and invasion detection systems, are often overlooked by well -designed social technical campaigns. These attacks include from simple frauds to complex models related to identity and fake theft.

University of Kabarak, like many organizations, faced continuous threats to try social techniques targeting students, teachers and staff. Understanding specific vulnerabilities and related vectors for university environment is very important to develop target defense mechanisms. Currently, the university is based on training to raise awareness of cybersecurity in general, but an adaptive and targeted approach is more necessary to approach the developing social technical context. This study will study the current cognitive status of social engineering in the university and will offer appropriate strategies to improve its recovery.

1.3 Problem Statement

The current cybersecurity landscape is increasingly challenged by sophisticated social engineering attacks that exploit human vulnerabilities. Kabarak University faces the following critical problems:

1. **Lack of Targeted Awareness:** Existing cybersecurity training is broad and may not adequately address the specific social engineering threats faced by university members.

2. **Insufficient Detection Mechanisms**: The university lacks advanced mechanisms for detecting and preventing social engineering attacks, making it difficult to identify and respond to ongoing threats effectively.

3. **Limited Understanding of Attack Impacts:** There is an incomplete understanding of the potential impacts of successful social engineering attacks, including data breaches, financial losses, and reputational damage.

These problems highlight the need for a comprehensive study to develop and implement targeted social engineering mitigation strategies at Kabarak University.

1.4 Objectives

1.4.1 Main Objective

The main objective of this project is to develop and implement a targeted social engineering awareness and mitigation framework for Kabarak University, enhancing the institution's resilience against social engineering attacks.

1.4.2 Specific Objectives

I. Investigate the common social engineering techniques used in attacks targeting universities and similar institutions, focusing on phishing, pretexting, and baiting.

II. Develop a customized social engineering awareness program for Kabarak University, incorporating interactive training modules and simulated phishing campaigns to improve user recognition of social engineering attempts.

III. Design and implement enhanced detection mechanisms for identifying and preventing social engineering attacks, including email filtering and behavioral analysis tools.

IV. Analyze the effectiveness of the implemented mitigation strategies through pre- and post-training assessments and simulated attack scenarios, measuring improvements in user awareness and system resilience.

1.5 Research Questions

1. What are the most prevalent social engineering techniques used in attacks targeting universities and similar institutions?

2. How can a customized social engineering awareness program be effectively developed and implemented to improve user recognition of social engineering attempts at Kabarak University?

3. What enhanced detection mechanisms can be designed and implemented to identify and prevent social engineering attacks targeting Kabarak University?

4. How effective are the implemented mitigation strategies in improving user awareness and system resilience against social engineering attacks at Kabarak University?

1.6 Significance of the Study

This study is significant for several reasons:

* **Enhanced Cybersecurity:** It provides practical strategies for improving the cybersecurity posture of Kabarak University by addressing the human element, which is often the weakest link in security systems.

* **Risk Reduction:** By developing targeted awareness programs and detection mechanisms, the project reduces the risk of successful social engineering attacks and their associated impacts.

* **Educational Contribution:** The research contributes to the broader understanding of social engineering threats and mitigation strategies in the context of higher education.

* **Timeliness:** Given the increasing sophistication and frequency of social engineering attacks, this study addresses a critical and timely need for enhanced cybersecurity measures.

1.7 Scope and Limitations of the Study

The scope of this study includes:

* **Focus Area:** The research will focus on social engineering attacks targeting Kabarak University.
* **Target Audience:** The study will involve students, faculty, and staff of Kabarak University.
* **Techniques Covered:** The research will cover common social engineering techniques such as phishing, pretexting, baiting, and impersonation.
* **Mitigation Strategies:** The project will develop and implement targeted awareness programs, detection mechanisms, and incident response protocols.
* **Timeframe:** The study will be conducted over a period of e.g., six months.

1.8 The limitations of this study **include:**

* **Limited Generalizability:** The findings may be specific to Kabarak University and may not be directly applicable to other institutions without adaptation.
* **User Participation:** The effectiveness of the awareness program depends on the participation and engagement of university members.
* **Evolving Threats:** Social engineering techniques are constantly evolving, and the implemented mitigation strategies may need to be updated to address new threats.

1.8 Proposed Modules

1. **Awareness Training Module:**
   * **Purpose:** Educate users on social engineering tactics.
   * **Functionality:** Interactive sessions, quizzes, and simulated attacks.
2. **Phishing Simulation Module:**
   * **Purpose:** Test user awareness.
   * **Functionality:** Sends simulated phishing emails and tracks responses.

3. Detection and Alerting Module:

* **Purpose:** Identify and flag suspicious activities.
* **Functionality:** Monitors email traffic, and user behavior.

4. Reporting and Analytics Module:

* **Purpose:** Provide insights on the effectiveness.
* **Functionality:** Generates reports on user awareness.

Chapter 2: Literature Reviews

2.1 Introduction

This chapter offers a complete assessment of existing documents on social techniques, including its techniques, impact and decline strategies. The Journal of Academic Research Test, Industry Report and Case Research to identify the main trends, the best practices and the gap in the current knowledge. The goal is to provide a solid basis for the proposed research by synthesizing existing knowledge and emphasizing the need to investigate more in the context of the University of Kabarak.

2.2 Social Engineering Techniques

2.2.1 Phishing

Phishing is a type of social technical attack in which the attacker sends fraud messages designed to encourage a person to reveal sensitive information or deploy toxic software on the victim's infrastructure (2019). Fraudulent attacks can be very effective because of the ability to exploit people's psychology, often use urgently or fear to encourage victims of action (Wombat security, 2018).

2.2.2 Pretexting

Fake implies that creating a script or an excuse is taken to persuade victims to provide information or take actions they often do not do (Mitnick and Simon, 2002). This technique is based on building trust with the victim, usually due to the appropriation of the wrong reference (Kumar et al., 2019).

2.2.3 Baiting

Bait related to providing something Atrithm, such as free download or USB readers with attractive labels, to attract victims into traps (Mitnick and Simon, 2002). When bait is done, the attacker can access the victim's system or data.

2.2.4 Quid pro

This technique is often used in scenarios in which an attacker pretends to be a service provider or a computer.

2.2.5 Tailgating

Tailgating implies an attacker to get unauthorized access to a restricted area by obeying an authorized person (Kumar et al., 2019). This technique uses physical security holes and may be especially difficult to prevent.

2.3 Impact of Social Engineering Attacks

2.3.1 Data Breaches

Social technical attacks often lead to data violations, in which sensitive information is infringed or stolen (Verizon, 2020). These violations can lead to significant financial loss and reputation for organizations.

2.3.2 Financial loss

Successful social attacks can lead to significant financial losses for individuals and organizations (Ponémon Institute, 2019). These losses may be the result of direct flights, legal fees and restoration efforts.

2.3.3 Reputation damage

Social technical attacks can harm the reputation of an organization and erode the trust of customers and stakeholders (Ponemon Institute, 2019). Rebuilding confidence after such incidents may be difficult and expensive.

2.4 Mitigation strategy

2.4.1 Cognitive raising training

Cognitive raising training is a major factor in protecting social engineering(technical), educating users about how to recognize and avoid social technical attacks. Effective training programs should include interactive sessions, tests and simulation attacks to start users and improve maintenance.

2.4.2 Technical Control

Technical control, such as email filtering and multi-employee authentication, can help prevent social technical attacks (Kumar et al., 2019). These controls can reduce the risk of successful attacks by limiting the roads that attackers can operate.

2.4.3 Reactions from incidents

Actually, having a problem of incident response is clearly defined to be effective to meet effectively and recover after social technical attacks (Verizon, 2020). This plan should include procedures for preventing, eradicating, recovery and after the incident.

2.5 Gaps in the Literature

Although there is an important literary store in social engineering, some space remains:

*** Specific research for the context:** There is a need more specific studies for threats of threats.

*** The effectiveness of training programs:** Additional research is necessary to evaluate the long - term effectiveness of social cognitive training programs and identify the best practices to design and implement these programs (Wombat Security, 2018).

*** Integrated technical and human control:** Requires more research on how to effectively integrate technical control measures and people to create a complete defensive strategy of social techniques (Kumar et al., 2019).

2.6 CONCLUSION

The literature review highlights the importance of social engineering as an important threat of cyber security and the need for effective impaired strategies. Current documents provide a solid basis for the proposed research, but there are also some shortcomings to fill. The study was proposed for the purpose of filling these gaps by developing and implementing a target framework to perceive and impair social techniques for the University of Kabarak, improving the recovery of the organization against social technical attacks.

Chapter 3: Research Methodology

3.1 Introduction

This chapter describes the research method will be used to study the threats of social engineering and develop strategies to minimize efficiency for the University of Kabarak. This method includes a combination of quantitative and qualitative research methods to collect data, analyze results and evaluate the effectiveness of proposed interventions. This chapter details research design, data collection method, sample population, data analysis technique and ethical consideration. The goal is to provide a clear and structured approach to answer research questions and achieve the goals of the research.

3.2 Research design

This research will use mixed methods, combining quantitative and qualitative research methods to provide full understanding of social technical threats and minimizing strategies. Research design includes the following stages:

- **Needs Assessment:** Conduct a survey to assess the current level of social engineering awareness among students, faculty, and staff at Kabarak University.
- **Intervention Development:** Develop a customized social engineering awareness program and implement enhanced detection mechanisms.
- **Evaluation:** Evaluation of the effectiveness of interventions performed by pre-training and post-training reviews, simulation attack scenarios and feedback surveys.

The integration of quantitative and qualitative methods will allow stronger and more nuanced understanding of research. Quantitative data will provide information that can be measured about the circulation ratio and the impact of social technical attacks, while the qualitative data will provide rich contextual information about user experience and perceptions.

3.3 Data Collection Methods

The following data collection methods will be used in this study:

Survey:

Managing questions before and after training to assess changes in social awareness between students, teachers and staff. Survey will include questions about social technical technical knowledge, attitude towards cybersecurity and self -pressure acts related to online security.

Investigating tool: A structured question will be designed to capture demographic information (age, gender, part, role), knowledge of social technical tactics, attitudes for network security acts and self -determining online security.

Administration: Survey will be conducted online using a safe platform (for example, Google Forms, Surveymonkey) to ensure security and ease of participation.

Pilot test: Investigating tools will be tested by a small group of participants to determine any ambiguity or problems before the general distribution.

Simulation fraud campaigns:

Carrying out simulation fraud campaigns to measure user sensitivity to social technical attacks before and after cognitive training. These campaigns will be involved in sending real frauds to a sub -set of university population and to follow the number of users clicking the link or providing sensitive information.

Phishing design: Actual scam emails will be designed to imitate common social technical tactics, such as urgent requirements, attractive provision or threats.

The target and followed: A subset of university population will be targeted and feedback for fraudulent emails will be monitored using specialized software.

Consider morality: Participants will be informed that they may suffer fraudulent attacks in the research framework.

Interviews:

Will explore the types of social technical attacks that have been observed at the University of Kabarak, the existing security measures and cognitive effectiveness of these measures.

Interview protocol: A semi -structural interview protocol will be developed to guide interviews, ensuring that the main subjects are mentioned while allowing flexibility to monitor.

Select participants: IT staff and security staff will be selected according to their experience and expertise on cybersecurity**.**

Write data and transcription: Interviews will be saved with the consent of the participants and the phonetic to analyze.

Document Analysis:

This analysis will provide a full overview of the university's current cyber security posture and will clarify the development of targeted minimizing strategies.

Determine the documents: Related documents will be determined by consulting IT staff and checking the university's online resources.

Content analysis: A systematic content analysis will be implemented to extract the main information about security policies, incident response processes and training programs.

Analysis of gaps: An analysis of gaps will be done to identify areas where current security measures of the university are missing.

The selection of these data collection methods is guided by research objectives and the need to collect quantitative data and qualitative data to meet the overall research issues.

3.4 Sample Population

The target population for this study includes all students, faculty, and staff at Kabarak University. A representative sample will be selected using stratified random sampling to ensure adequate representation from different departments and roles within the university. The sample size will be determined based on statistical power analysis to ensure the validity and reliability of the findings.

3.4.1 Sampling Strategy:

Stratification: The population will be stratified based on the following characteristics:

Role: Students, Faculty, Staff

Department: Academic Departments, Administrative Departments, IT Department

Random Sampling: Within each stratum, participants will be randomly selected to ensure that the sample is representative of the population.

Sample Size Justification: The rationale for selecting a stratified random sample is to ensure that all subgroups within the university are adequately represented in the study, which enhances the generalizability of the findings.

3.4.2 Sample Size Determination:

The sample size will be determined using statistical power analysis to ensure that the study has sufficient power to detect meaningful effects. The following parameters will be considered:

Significance Level: $\alpha = 0.05$

Power: $1 - \beta = 0.80$

Effect Size: A moderate effect size (e.g., Cohen's d = 0.5) will be assumed based on previous research in this area.

Based on these parameters, the required sample size will be calculated using appropriate statistical software or formulas.

Sample Size Table:

Stratum	Population Size	Sample Proportion	Sample Size
Students	8000	0.9835	361
Faculty	8	0.00098	1
Staff	126	0.0155	6
Total	8134		368

Note: The sample sizes will be calculated based on the population sizes and desired statistical power.

3.5 Data Analysis Techniques

The data collected in this study will be analyzed using the following techniques:

Quantitative Analysis: Use descriptive statistics (e.g., mean, standard deviation) and inferential statistics (e.g., t-tests, ANOVA) to analyze survey data and compare pre- and post-training scores. The statistical software package SPSS will be used for data analysis.

Descriptive Statistics: Calculate means, standard deviations, frequencies, and percentages to summarize the characteristics of the sample and the distribution of variables.

Inferential Statistics: Use t-tests to compare pre- and post-training scores on the knowledge and awareness surveys. ANOVA will be used to compare scores across different groups (e.g., students, faculty, staff). Chi-square tests will be used to analyze categorical data.

Regression Analysis: Regression analysis will be used to explore the relationship between demographic variables (e.g., age, gender, department) and social engineering awareness.

Qualitative Analysis: Use thematic analysis to analyze interview transcripts and identify key themes and patterns related to social engineering threats and mitigation strategies. Thematic analysis will involve the following steps:

Transcription: Transcribe the interview recordings verbatim.

Coding: Develop a coding scheme based on the research questions and relevant concepts.

Theme Identification: Identify recurring themes and patterns in the data.

Interpretation: Interpret the themes and patterns in the context of the research questions.

Software Support: NVivo or similar qualitative data analysis software will be used to facilitate the coding and analysis process.

Mixed-Methods Integration: Integrate quantitative and qualitative findings to provide a comprehensive understanding of the research questions. This will involve triangulating the data from different sources to identify areas of convergence and divergence.

Data Triangulation: Compare and contrast the findings from the surveys, phishing simulations, interviews, and document analysis to identify areas of convergence and divergence.

Narrative Synthesis: Develop a narrative synthesis to integrate the quantitative and qualitative findings, providing a rich and nuanced understanding of the research problem.

The integration of quantitative and qualitative findings will allow for a more nuanced and comprehensive understanding of the research problem.

3.6 Research Ethics

This study will adhere to the following ethical principles:

- **Enlightenment agreement:**
- Obtained the consent of all participants before their implications in the study. The agreement process will include providing participants of the research goals, related procedures, risks and potential advantages and their right to withdraw money at any time.
- **Form agreed:** A sample agreed in detail will be developed, describing the goals of research, procedures, risks and potential advantages, security measures and voluntary nature of participation.
- **Document:** The signed forms will be taken from all participants before they participate in the research.
- **Security:** Protects the security of participants by hiding data and by storing it safely. All data will be stored in the computer protected by password and will only be accessible to the search team.
- **Anonymous:** names of participants and other identification information will be deleted from data.
- **Data security:** data will be stored in a safe computer and protected by password and will only be accessible to the search team.
- **Safe data transfer:** All electronic data will be encrypted to protect security.
- **Voluntary participation:** Ensures that participating in the research is voluntary and participants have the right to withdraw money at any time. Participants will be informed that they can withdraw from research at any time without being punished.
- **The right to withdraw money:** participants will be notified of the right to withdraw from the study at any time without being fined.
- **No forced:** without forced or pressure will be used to encourage participation.

- **Beneficiaries:** Maximize the advantages of the study while reducing risks or potential damage to participants. The potential advantages of research include better awareness of cybersecurity and reducing sensitivity to social technical attacks.
- **Risk assessment:** Risk assessment in the situation will be done to determine the hidden risks for participants.
- **Dit -down strategy:** Strategies will be done to minimize hidden risks, such as providing discussions after simulating fraudulent attacks.
- **Justice:** Ensures the fair and fair choice of participants and the advantage distribution.
- **Fair options:** Participants will be selected by using multi -layer random sampling methods to ensure that all small groups of the university are shown.
- **Fair distribution by the advantages:** Advantages of the study (for example, better awareness of cybersecurity) will be provided to all members of the university community.
- **Respect for Persons:** Treat all participants with respect and dignity, and protect their autonomy.
- **Privacy Protection:** Participants' privacy will be protected at all times.
- **Cultural Sensitivity:** The study will be conducted in a culturally sensitive manner, taking into account the diverse backgrounds of the participants.
- **Institutional Review Board (IRB) Approval:** Seek approval from the Kabarak University IRB before commencing the study. The IRB will review the research protocol to ensure that it adheres to ethical guidelines and protects the rights and welfare of participants.
- **IRB Submission:** A detailed research protocol will be submitted to the Kabarak University IRB for review and approval.
- **Compliance:** The study will be conducted in accordance with the IRB's guidelines and recommendations.

Adherence to these ethical principles will ensure that the study is conducted in a responsible and ethical manner.

3.7 Conclusion

The research methodology outlined in this chapter provides a systematic and rigorous approach to investigate social engineering threats and develop effective mitigation strategies for Kabarak University. By combining quantitative and qualitative research methods, this study aims to provide a comprehensive understanding of the research questions and contribute to the development of a targeted social engineering awareness and mitigation framework for the university. The ethical considerations outlined in this chapter will ensure that the study is conducted in a responsible and ethical manner, protecting the rights and welfare of the participants.

References

Kumar, S., Singh, M., & Singh, S. K. (2019). Social engineering attack detection using machine learning. *Journal of Intelligent Information Systems*, 54(2), 287–305. doi: 10.1007/s10844-018-0524-4

Mitnick, K. D., & Simon, W. L. (2002). Ghost in the wires: My adventures as the world's most wanted hacker. Little, Brown and Company.

Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. IBM Security.

Verizon. (2020). 2020 Data Breach Investigations Report. Verizon Enterprise Solutions.

Wombat Security. (2018). 2018 Beyond the Phish Report. Wombat Security Technologies.