**AI-Based Phishing Email and Website Detection System using OpenAI Language Model**

**Chilton Keith Simiyu**

**CNS**

**Supervisor Name**

**Victor Rop**

**Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer Networks and Cybersecurity at the Strathmore University**

**School of Computing and Engineering Science Strathmore University**

**Nairobi, Kenya**

**May 2024**

# Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student Name: Chilton Keith Simiyu Admission Number:147478

Student Signature: Date:

The Proposal of **Chilton Keith Simiyu** has been reviewed and approved by **Mr.** **Victor Rop**

Supervisor Signature: Date:

# Ackn**owledg**ement

I would like to thank my supervisor for his guidance, expertise, experience and unwavering support during the whole project writing and implementation process. I would also like to express my deepest gratitude to my parents for their support and guidance, which have been pivotal in my journey in school. Their endless love, encouragement, and sacrifices have been my driving force. Thank you for believing in me and standing by my side throughout this journey in school. I would also like to thank my friends and classmates for their support in school and home, for pushing me every time and helping me anytime I was stuck. Thank you all.

# Abstract

With the significant growth of internet usage today, the threat of phishing attacks has grown rapidly, stealing personal information, evading privacy and financial security. Phishing has evolved into a sophisticated cybercrime, exploiting users' trust and deceiving them into giving out sensitive data to attackers without knowing it. This project aims to use the power of AI models such as GPT and Open AI language APIs to develop a robust system for detecting phishing emails and websites.

The proposed system will analyze email headers and content, using natural language processing techniques to distinguish between legitimate communications and phishing attempts. It will give users the ability to scan URLs and emails enabling the system to provide detailed assessments of website authenticity and potential phishing indicators.

Table of Contents

[Declaration and Approval ii](#_Toc167093756)

[Acknowledgement iii](#_Toc167093757)

[Abstract iv](#_Toc167093758)

[List of Figures vi](#_Toc167093759)

[List of Abbreviations vii](#_Toc167093760)

[Chapter 1: Introduction 1](#_Toc167093761)

[1.1 Background Information 1](#_Toc167093762)

[1.2 Problem Statement 2](#_Toc167093763)

[1.3 Objectives 2](#_Toc167093764)

[1.3.1 General Objectives 2](#_Toc167093765)

[1.3.2 Specific Objectives 2](#_Toc167093766)

[1.4 Research questions 2](#_Toc167093767)

[1.5 Justification 3](#_Toc167093768)

[1.6 Scope and Limitations 3](#_Toc167093769)

[1.6.1 Limitations 4](#_Toc167093770)

[1.7 Delimitation 4](#_Toc167093771)

[Chapter 2: Literature Review 5](#_Toc167093772)

[2.1 Introduction 5](#_Toc167093773)

[2.3 Related Works 5](#_Toc167093774)

[2.3.1 DNS Filtering 5](#_Toc167093775)

[2.3.2 Machine Learning 6](#_Toc167093776)

[2.3.3 Signature-based Detection 7](#_Toc167093777)

[2.3.4 User Training and Awareness 7](#_Toc167093778)

[2.4 Research gaps 7](#_Toc167093779)

[2.5 Empirical Framework 8](#_Toc167093780)

[2.6 Conceptual Framework 8](#_Toc167093781)

[Chapter 3: Methodology 10](#_Toc167093782)

[3.1 Introduction 10](#_Toc167093783)

[2.2 Methodology 10](#_Toc167093784)

[3.3 Justification 13](#_Toc167093785)

[3.4 Deployment and Rollout 14](#_Toc167093786)

[3.5 Ongoing Maintenance and Updates 14](#_Toc167093787)

[3.6 List of Design Diagrams 14](#_Toc167093788)

[3.7 List of development tools that will be used 14](#_Toc167093789)

[Reference 16](#_Toc167093790)

[Appendices 19](#_Toc167093791)

[Appendix 1 19](#_Toc167093792)

[Literature Review/Related Work 21](#_Toc167093793)

[Methodology 21](#_Toc167093794)

[Proposal Presentation 21](#_Toc167093795)

[Total Marks 21](#_Toc167093796)

# List of Figures

[Figure 1.1: Machine Learning model 6](#_Toc167093898)

[Figure 2.1: Conceptual Framework 9](#_Toc167093899)

[Figure 3.1: A graph of phishing attacks 13](#_Toc167093900)

# List of Abbreviations

GPT – Generative Pre-trained Transformers

AI – Artificial Intelligence

LLM – Large language models

ML – Machine Learning

NLP - natural language processing

URL – Uniform Resource Locator

DNS – Domain Name System

SVM Support vector machine

# Chapter 1: Introduction

# 1.1 Background Information

Phishing attacks have become a persistent threat in today's digital landscape due to the advance and rapid change in technology. Phishing is a type of social engineering attack used by attackers to steal user data, including login credential, credit card numbers and other personal information. The user is tricked into clicking a malicious link in the email they receive or website, which can lead to the installation of malware or viruses to the user’s computer. Phishing sites are websites that aim to steal personal information or money, or to cause malware infections by luring users into clicking malicious links. Attackers also use emails, short message service (SMS), and web advertisements to attract users and redirect them to phishing sites by having them click on malicious links. (Vaishnavi,2018)

The evolution of phishing tactics has made them increasingly sophisticated and difficult to detect using traditional security measures alone. Cybercriminals leverage various techniques now, including social engineering, spoofed domains, and persuasive language, to trick unsuspecting victims into revealing confidential information. As a result, there is a pressing need for advanced and proactive solutions that can effectively find and mitigate phishing threats.

Artificial intelligence (AI) and machine learning (ML) technologies have emerged as powerful tools in the fight against cyber threats, including phishing attacks. Security analyst have started using this new technology to try and curb attacks such as phishing, MITM because of its ability to learn and adapt on their own. AI models, such as OpenAI's Generative Pre-Trained Transformer (GPT) language model, have demonstrated remarkable capabilities in natural language processing (NLP) tasks, understanding problems, and contextual analysis of problems and providing solutions to these problems. These AI models can be trained on vast amounts of datasets to recognize patterns, anomalies, and malicious intent in emails and links. This has made these models valuable assets in enhancing cybersecurity defenses over the internet. Using deep learning capabilities of models like GPT, organizations can augment their existing security infrastructure with intelligent threat detection mechanisms such as using AI for log analysis. These techniques are unique and important in keeping up with the new tactic’s attackers keep evolving every day (Alhogail, 2021).

# 1.2 Problem Statement

Phishing attacks remain a significant cybersecurity threat, with attackers constantly evolving their tactics to bypass traditional detection methods. Current solutions often struggle to keep up with the sophisticated techniques being used by the attackers nowadays due to the rapid change in technology and innovation of AI, leading to an increasing number of successful phishing incidents on the internet. In 2022, around 30 percent of adults worldwide encountered phishing scams and in the fourth quarter of 2022, there were over 1.35 million unique phishing sites worldwide. This not only compromises sensitive information which causes big loses to this companies but also damages the trust and reputation of organizations and individuals. The lack of robust mechanisms for identifying phishing emails and websites poses a critical challenge in ensuring cyber resilience and data security. Phishing can be severe, leading to data breaches, financial losses, and reputational damage.

# 1.3 Objectives

# 1.3.1 General Objectives

This project aims to develop and implement an AI-based Phishing Detection System using OpenAI's Language Model for both emails and websites. I am to enhance cybersecurity defenses by creating an automated system capable of efficiently detecting phishing emails and websites.

# 1.3.2 Specific Objectives

1. Conduct a comprehensive analysis of existing phishing detection methods and their limitations.
2. Develop an advanced GPT-based model specifically tailored for detecting phishing emails and websites.
3. Implement and optimize the detection system to ensure accurate identification of phishing attempts.
4. Evaluate the performance and efficiency system through extensive testing and validation against a diverse range of phishing scenarios.

# 1.4 Research questions

1. How effective is OpenAI's language model in detecting phishing emails compared to other systems?
2. What are the key features that distinguish phishing emails from legitimate ones, and how accurate are these features?
3. What are the limitations and challenges of using AI for phishing detection?
4. How can AI-based phishing detection systems be integrated into organizational cybersecurity policies and practices to improve overall security against phishing attacks?

# 1.5 Justification

Organizations have tried to mitigate this attack by using different ways such as employee training, using spam filters and using MFA but the attackers still find a way to bypass this. My proposed solution involves using the latest model of OpenAI, particularly GPT-4 and other language models to enhance phishing detection capabilities from websites and emails. By training the model on a vast dataset of phishing emails and websites, I aim to create a robust system capable of identifying patterns for phishing attempts on both emails and websites. My proposed solution will be web-based and it will be using GPT to interact with the user, where one will be able to connect it to their email and it will scan for phishing emails and provide a detailed insight of its findings. It will allow the user ask questions about the email’s information such as the header files and source. The model will also allow users to paste a URL and the model will check if the URL pasted is authentic or it’s a phishing website.

# 1.6 Scope and Limitations

This project will involve a number of steps to make everything promised possible. This includes the creation of algorithms capable of analyzing email content to detect phishing attempts including identifying common patterns, sender information, and malicious intent indicators for detection. This project also extends to detecting phishing websites by analyzing URL structures, DNS information, webpage content, and visual elements using machine learning and web analysis techniques to find this URLs with malicious intent. This will involve integration of OpenAI's language model to enhance the system's capabilities in natural language processing for identifying common patterns and analyze them. This project will use specifically the language model called GPT-4 to help user interact well with the model. This project also applies machine learning and data analysis for model training which will help the model identify patterns, learn the difference between a phishing email and phishing URL from a legitimate URL and email. (Pandiyan,2021)

## 1.6.1 Limitations

Developing and training AI models for phishing detection requires a lot of knowledge about AI, coding, web scripting, resources and expertise in machine learning. There are a few limitations hindering this project to perfection. These limitations include:

1. Limited and Imbalanced Data: Obtaining a diverse and well-labeled dataset for training a phishing detection system can be challenging. Additionally, the distribution of phishing and legitimate instances in the dataset may be imbalanced, leading to bias in the model's performance.
2. Evolving Phishing Techniques: Phishing attacks continually evolve and adapt, making it challenging to keep detection systems up to date. New phishing techniques, such as spear phishing or social engineering tactics, require constant monitoring and updating of the training data and models.

## 1.7 Delimitation

Though a few limitations are expected during the implementation of this system, there are a few countermeasures I will do to try and prevent these limitations. They include:

1. Creating and using my own dataset to avoid using already made datasets.
2. Using the latest AI models to try and keep up with the evolving phishing attacks.

# Chapter 2: Literature Review

# 2.1 Introduction

Systems and tools that use Artificial Intelligence have gained a significant attention in the field of cybersecurity since the world is evolving and developing rapidly from traditional ways of manually doing everything to now using AI where you get to train it to do certain tasks and it does it with ease, perfections, fast and you can rely on them. This literature review aims to provide a comprehensive analysis of existing works related to Artificial Intelligence and phishing detection tools, highlighting their similarities, differences, and contributions. By examining the different frameworks outlined, this review identifies key theories, research topics, and relevant studies to establish a strong foundation for my project.

# 2.3 Related Works

Due to the evolving and changing of cyber-attacks such as phishing because the attackers are using better tools and techniques, there have been need for new ways to detect phishing attacks. There are many techniques being used now by companies and organizations to try and curb these phishing attacks and keep up with the attackers. These techniques include:

## 2.3.1 DNS Filtering

DNS filtering is a technique that blocks access to known malicious domains and IP addresses associated with phishing campaigns. It operates at the DNS (Domain Name System) level, where domain names are translated into IP addresses. DNS filtering services maintain databases of known malicious domains and IP addresses, often updated in real-time, to identify and block access to these sites. By redirecting users away from malicious sites, DNS filtering helps prevent successful phishing attacks. If a user attempts to access a website known for hosting phishing content, the DNS filtering service intercepts the DNS request and returns a block page or redirects the user to a safe page, thereby protecting the user from potential phishing attempts (Armstrong et al., 2015).

## 2.3.2 Machine Learning

ML approaches are popular for phishing websites detection and it becomes a simple classification problem. Machine learning algorithms are widely used for detecting phishing emails and websites. These models are trained on labeled datasets containing examples of phishing and legitimate content. During training, the algorithms learn to identify patterns and anomalies associated with phishing behavior, such as suspicious content, unusual sender characteristics, and deceptive website elements.

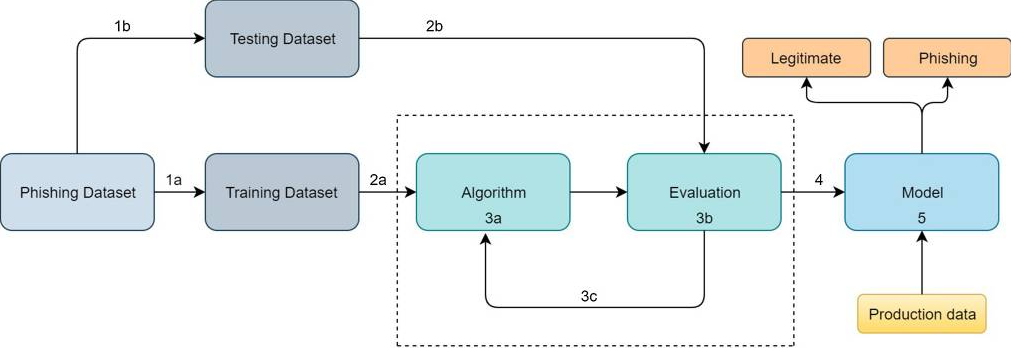


Figure 1.1: Machine Learning model

To train a machine learning model for a learning-based detection system, the data at hand must-have features that are related to phishing and legitimate website classes. Different classifiers are used to detect a phishing attack. Previous studies show that detection accuracy is high as robust ML techniques are used. Several feature selection techniques are used to reduce features. Figure 1 shows the working of the machine learning model. A batch of input data is given as input for training to the machine learning model to predict the phishing attack or legitimate traffic (Ismail, 2020).

Supervised learning models are trained using labeled data, where each sample is labeled as either phishing or legitimate. These models learn to classify new instances based on features extracted from the data. On the other hand, unsupervised learning models do not require labeled data and can identify patterns and outliers in the data, making them suitable for detecting previously unseen phishing tactics. Machine learning-based phishing detection systems often employ feature extraction techniques to capture relevant information from emails or webpages, such as email headers, content analysis, URL characteristics, sender information, and behavioral patterns. By analyzing these features, machine learning models can accurately detect phishing attempts with high precision and recall (Aljawarneh et al., 2020).

## 2.3.3 Signature-based Detection

Signature-based detection relies on creating signatures or patterns based on known phishing attacks. These signatures can include specific keywords, email header information, URL characteristics, or malicious file attachments commonly attached and included in phishing attempts. Email filters and security software compare incoming emails or website URLs against these signatures to identify and block phishing attempts. While signature-based detection is effective for known phishing attacks and provides rapid detection, it may struggle with new or sophisticated phishing tactics that do not match existing signatures. Attackers can modify their techniques, such as using polymorphic malware or obfuscating URLs, to evade signature-based detection systems. Therefore, while valuable, signature-based detection should be complemented with other techniques for comprehensive phishing protection (Schultz et al., 2001).

## 2.3.4 User Training and Awareness

Educating users about phishing techniques and safe browsing practices is a proactive approach to phishing prevention. Training programs and simulated phishing exercises can significantly improve user awareness and reduce phishing attack incidences in organizations. Users are taught how to recognize common phishing indicators, such as suspicious email senders, unfamiliar URLs, requests for sensitive information, and urgency or scare tactics.

Training programs often include interactive modules, real-world examples of phishing emails, and guidance on how to verify the authenticity of emails and websites. Simulated phishing exercises involve sending simulated phishing emails to employees to assess their response and provide immediate feedback on phishing awareness levels. By raising awareness and fostering a culture of cybersecurity vigilance, user training and awareness programs empower individuals to be the first line of defense against phishing attacks, complementing technical security measures (Adams et al., 2018).

# 2.4 Research gaps

These techniques listed above are good and most of them work well but theirs is still a gap to be addressed, that’s where this project comes in. Signature-based detection is effective for known phishing attacks and provides rapid detection, it struggles with new or sophisticated phishing tactics that do not match existing signatures known to the database. Attackers can modify their techniques, such as using polymorphic malware or obfuscating URLs, to evade signature-based detection systems. Therefore, while valuable, signature-based detection should be complemented with other techniques for comprehensive phishing protection. Integrating human expertise into AI systems and researching hybrid approaches can enhance detection accuracy. Cross-platform phishing detection strategies, standardized evaluation metrics, and dataset training are essential for comprehensive threat coverage and objective performance assessments. Most of these techniques don’t take full advantage of the new AI models which attackers keep changing tactics and techniques they use, the techniques we have still fall behind and are not utilizing the new technology to its fullest.

# 2.5 Empirical Framework

This project enables researchers to comprehend the various methods, challenges, and trends for phishing attack detection. Nowadays, prevention from phishing attacks is considered a tough job in the system security domain. An efficient detection system ought to have the option to identify phishing attacks with low false positives. With high computational expenses, heuristic and data mining methods have high False positive rates, however better at distinguishing phishing attacks. The ML procedures give the best outcomes when contrasted with different strategies. A portion of the ML procedures can identify these attacks up to 99%. As malicious URLs are created every other day and the attackers are using techniques to fool users and modify the URLs to attack. Nowadays deep learning and machine learning methods are used to detect a phishing attack. classification methods such as SVM, C4.5 are also common. These methods are most useful and effective for detecting the phishing attacks.

# 2.6 Conceptual Framework

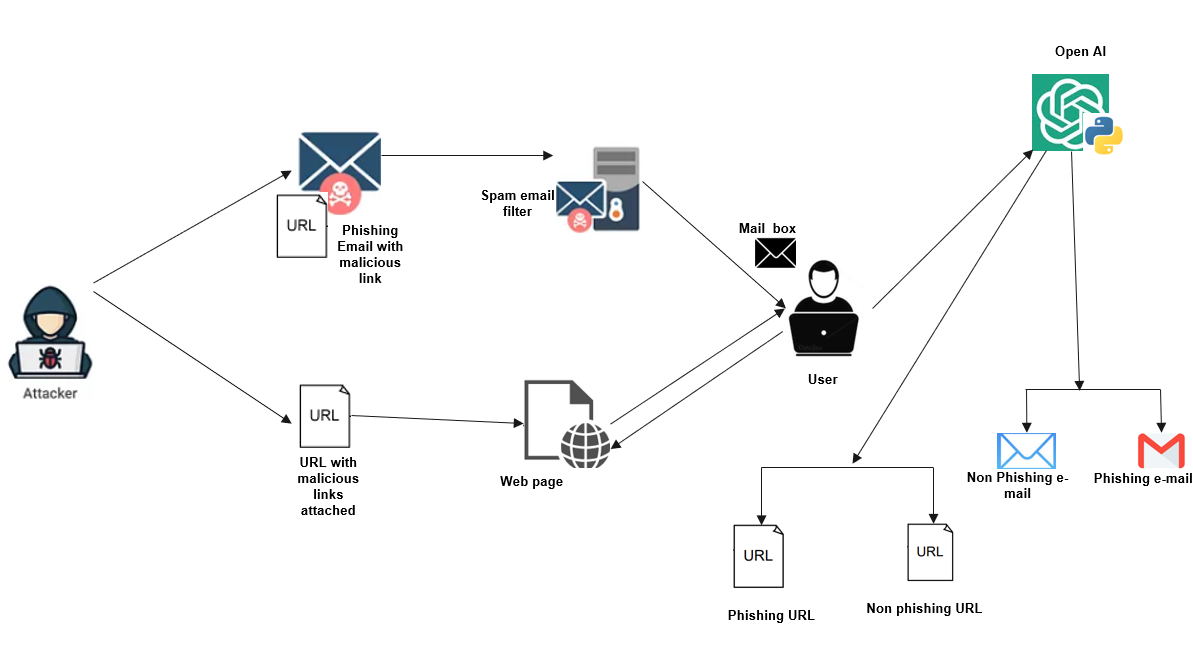


Figure 2.1: Conceptual Framework

Figure 2 Shows a conceptual framework of how the system will work. How it will react incase there’s a phishing attack either via email or a phishing URL. If an attacker sends a phishing email or URL, it will go to the user’s mailbox. Most of these phishing emails nowadays are able to bypass the spam email filters. Here is where the user is going to use the model to scan if the email is legitimate or fake. Using the openAI ChatGPT model, the user can ask the model to scan the email or URL to see if its legitimate. The model will display its finding to the user and explain everything to the user.

# Chapter 3: Methodology

# 3.1 Introduction

In this chapter, the methodology employed for conducting the research on an AI-Based Phishing Email and Website Detection that leverages the OpenAI Language Model will be outlined. This chapter aims to provide a clear understanding of the approach to be taken to achieve the objectives effectively and implement the system.

# Methodology

A typical email is composed of a header and a body. The email header has a specific structure consisting of several information related to the sender and the receiver, including their IP addresses, the subject, and the date. Regarding the email body, it has no specific format, and it can be customized and different from one email to another. However, there are some items that can be found in any typical email, such as text, link to a website, attached files, and the email's signature. Since not the entire email content is relevant in detecting legitimate emails from malicious ones, it is important to select and extract only those specific features that are used in phishing emails.

These features include: sender email address, attached file extension, blacklist keywords, secure socket layer (SSL) certificate, certificate authority (CA), redirection URL, hiding links, clear IP address, website traffic, and webpage age. Individual features may not reveal the legitimacy of an email but combining several features increase the likelihood of detecting potential phishing emails. These features include:

1. SSL certificate

When a user is requested to enter confidential data on legitimate websites, the exchanged data between the server and the end-user is encrypted, which can be achieved through the HTTP protocol with an additional secure socket layer. However, most of the phishing emails include HTTP links without any supplementary secure layer exposing the data to potential unauthorized access and loss. Thus, if an email includes a secure HTTP link, then it is legitimate; otherwise, it is malicious.

1. Certificate authority

Not every HTTPS link can guarantee a secure connection to the server and make the sensitive data undisclosed to a third party since the SSL certificate can be delivered by an unauthentic entity or self-signed. An SSL certificate is insufficient to decide if an HTTSs link is secure. Investigating the identity of the entity that issued the certificate is crucial in verifying the email's legitimacy. Thus, if an SSL certificate is not delivered by a trusted and credible authority such as GoDaddy, Comodo, and Symantec, then the email is suspicious and can be malicious.

1. Blacklist keywords

Phishing emails share in common some keywords and short phrases. These keywords have a sense of urgency, including "Click Now", "Verify Now," "Valid in 24h", and "Update Now." Including such keywords in the email, the body provides clues about the illicitness of the email. There are several suspicious keywords used by the attackers to grab the attention of the victim If the email includes one or more blacklist words, then it is malicious.

1. Redirection URL

Some phishing emails include a link that implicitly redirects the user to a hidden server before reaching the requested website, such as a proxy server. This server will handle the communication between the user, the malicious, and the legitimate websites. I will use GET request of the HTTP protocol to verify the legitimacy of an URL.

1. Hiding links

An alternative way to hide the actual URL website is to use hiding links, which rely on two techniques: URL shorteners and customized HTML emails. During an attack, the attacker wraps the real URL in a short one such as "goo.gl", or "j.mp". The attacker forges a HTML email with CSS and JavaScript scripts to customize the webpage link with a personalized clicked text or image. Thus, an email is suspicious if it includes a short URL.

1. Clear IP address

Some phishing emails include links with a clear IP address. "https://50.10.125.26/index.php" is an example that indicates the illegitimacy of the email. Using an IP address instead of the specific domain name is because malicious webpage links last for less than three days, and attackers do not buy a domain name for a short period of time. Thus, if a link includes a clear IP address, then it is suspicious.

1. Website traffic

Legitimate websites receive a number of requests with a specific traffic rate per day. A legitimate website has a rank less or equal to 150,000 in the Alexa database. However, phishing websites are not often visited as they have a short lifetime, and their traffic is low.

1. Age of the webpage

Since most phishing webpages have a short lifetime, the age of the webpages can provide information about their legitimacy. The age of the authentic website is usually more than one year. Therefore, if the email includes a webpage link with less than one year, then it is suspicious.

1. Sender’s email address

In some phishing emails, there is an inconsistency between the email subject and the address of the sender. For instance, some malicious emails seem to be emitted by an authentic entity, such as Microsoft or Dropbox, since the email's subject states something similar to "the user X has shared some files with you" or "Reinitialize the password." However, the sender's email address includes a strange domain name such as "@sharing.dboxfile.com" or "@dropbox.com." Thus, such inconsistency can be relevant in detecting malicious senders. Thus, if a domain name does not belong to the credible domain names list, then the email is suspicious.

1. Attached file extension

It is used to increase the likelihood of detecting phishing emails. Some phishing emails include an attached file, including an embedded payload. This payload can be an executable shell script giving the attacker the privileges to execute some command on the user's machine. One of the known tools used by attackers to forge phishing emails is the social engineering Toolkit installed by default on the Kali Linux. It generates a file including the payload with ".exe" or ".dll" extension. If the attached file has ".exe" extension, then the email is suspicious.

Using all these features I will be able to train the model on how to identify these abnormalities and find phishing emails. Using only one won’t be effective, but combining all these features I will be able to identify malicious emails with malicious intents.

# 3.3 Justification

The graph below shows the rapid increase in phishing attacks since the rapid growth of technology over the years. There is need to employ the above techniques and try and minimize and prevent these attacks since they have become more sophisticated and not easy to identify

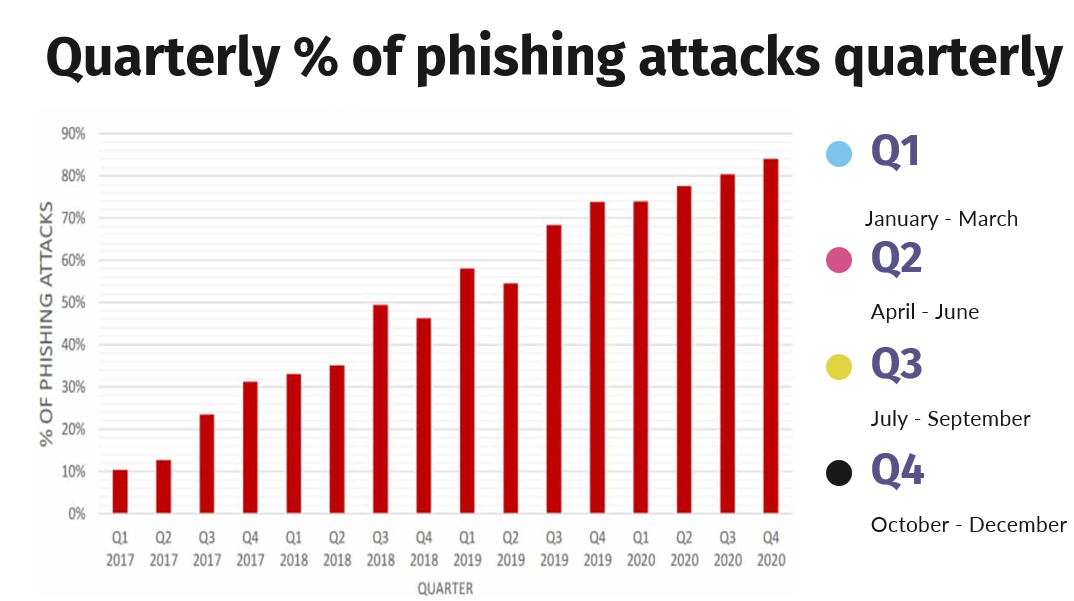


Figure 3.1: A graph of phishing attacks

# Deployment and Rollout

Once the tool has been validated, it is deployed on the internet where users can assess the website from anywhere over the internet and use the tool to scan for malicious emails and scan URLs. The website will have user friendly interface that allows users interact with the model.

# Ongoing Maintenance and Updates

I will always be updating the website with the most recent security standards and device configurations and I will regularly monitor it for vulnerabilities in case a configuration wasn’t done properly. Additionally, periodically review and revise security policies and assessment standards as necessary. I will always make sure the website is safe for users and it works properly as said.

# List of Design Diagrams

*Figure 2* provides an overview of the system's objects, their properties, and how they are related, enabling a better understanding of the system's structure. It also shows how they will work and the flow of events incase of a phishing attack.

# 3.7 List of development tools that will be used

For the development of this project, there are a few software and hardware requirements needed to make this system. These requirements include:

* OpenAI API: OpenAI provides APIs for developers to use their OpenAI's language model and API for natural language processing tasks, such as analyzing email content and website information.
* Python: Python programming language will be used for developing AI models, implementing machine learning algorithms, writing the rules for the model, and integrating AI functionalities into the detection system.
* Machine Learning Libraries: Utilize libraries such as TensorFlow, PyTorch, or Scikit-learn for building and training machine learning models for phishing detection.
* Data Preprocessing Tools: I will employ tools like NLTK (Natural Language Toolkit) or spaCy for preprocessing textual data.
* Datasets – I will also need datasets to train the model on which emails are phishing emails and which ones are legitimate ones.
* Version Control: I will use Git and platforms like GitHub or GitLab for version control of code, collaboration, and tracking changes throughout the development process.
* IDE (Integrated Development Environment): I will use IDEs such as PyCharm, Jupyter Notebook, and Visual Studio Code for code writing, debugging, and experimentation with AI models.
* Web hosting - I will also need a web hosting for the website where people will interact with the model.
* Domain – I will need to buy a domain for our website.
* Web Development Tools: I developing a phishing website detection component, use web development tools like HTML, CSS, JavaScript, and frameworks like Flask or Django for building web interfaces and backend functionalities.

# Reference

Alhogail, A. (2021). Applying machine learning and natural language processing to detect phishing email. https://www.sciencedirect.com/science/article/pii/S0167404821002388

Belani, R., & Higbee, A. (2015). PhishMe Enterprise Phishing Susceptibility and Resiliency Report. https://technology-signals.com/wp-content/uploads/download-manager-files/PhishMe\_Enterprise\_Phishing\_Susceptibility\_and\_Resiliency\_Report.pdf

Haynes, K. (2021). Lightweight URL-based phishing detection using natural language processing transformers for mobile devices. https://www.sciencedirect.com/science/article/pii/S1877050921014368

Ismail, M. (2020). Comparative Performance of Machine Learning Methods for Classification on Phishing Attack Detection. https://www.researchgate.net/publication/344448999\_Comparative\_Performance\_of\_Machine\_Learning\_Methods\_for\_Classification\_on\_Phishing\_Attack\_Detection

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. https://www.researchgate.net/publication/220424040\_Social\_phishing

OpenAI. (n.d.). GPT-3 API Documentation. https://platform.openai.com/docs/api-reference/gpt-3

Ojewumi, T. (2022). Performance evaluation of machine learning tools for detection of phishing attacks on web pages. https://www.sciencedirect.com/science/article/pii/S2468227622000746

Pandiyan, S. (2021). Phishing attack detection using Machine Learning. https://www.sciencedirect.com/science/article/pii/S2665917422001106

The Anti-Phishing Working Group. (2022). Phishing Activity Trends Report: Q3 2022. https://docs.apwg.org/reports/apwg\_trends\_report\_q3\_2022.pdf

Vaishnavi, B., Aditya, K., & Shabnam, S. (2018). Study on Phishing Attacks. https://www.researchgate.net/publication/329716781\_Study\_on\_Phishing\_Attacks

Vemuri, N. (2023). Enhancing Human-Robot Collaboration in Industry 4.0 with AI-Driven HRI. Enhancing Human-Robot Collaboration in Industry 4.0 with AI-Driven HRI, 47(4). https://doi.org/10.52783/pst.196

Kalla, D., Samaah, F., Kuraku, S., & Smith, N. (2023). Phishing Detection Implementation Using Databricks and Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4452780

Nyathani, R. (2021). Innovations in HR: Harnessing the Power of AI and Cloud Solutions. https://doi.org/10.21275/SR231116142023

Vemuri, N. V. (2024). DevOps for Telehealth Services: Accelerating Deployment and Scalability. International Journal on Recent and Innovation Trends in Computing and Communication, 12(1), 160–163. <https://doi.org/10.17762/ijritcc.v12i1.9894>

# Appendices

## Appendix 1

**Strathmore University**

**School of Computing and Engineering Sciences**

**Project Proposal Assessment Guide**

|  |  |
| --- | --- |
| **Student Number** |  |
| **Working Title:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Evaluation Areas** | **Weight** | **Score** | **Notes** |
| **Title page:**  Informative, concise, and appropriate | **2 pts** |  |  |
| **Abstract**  To have background, problem, solution, methodology (approach data and tools) outcomes and expectations | **2 pts** |  |  |
| **Introduction**  Background **(2)**  *A clear illustration of issue, context and audience*  Problem Statement **(2)**  *Pain points, audience, who is affected and how solution comes in to fix the pain.*  Objectives (S.M.A.R.T and Linked to Problem Statement) **(2)**  Research questions **(1)**  *Alignment of questions with objectives*  Justification **(2)**  *Should be research supported.*  Scope of Project **(2)**  *Specify boundaries of people process, HW/SW, data etc.*  Limitations **(1)**  *Challenges Expected*  Delimitation **(1)**  *To do to counter anticipated challenges* | **(13 pts)** |  |  |
| Literature Review/Related Work Objectives mapping to Literature Review **(2)**  Critique of Theoretical framework and content adequacy (**2**)  *Principles, parameters of consideration*  Discussion of technologies contextualization for the proposed work **(2)**  Citations of content  and alignment to work **(2)**  Review of at least 3 systems comprehensively the working behind it **(2)**  Gaps identification, analysis relative to the proposed solution **(1)**  Conceptual Framework clear to communicate how it works, data flows, processing, actors **(3)**  *Diagram that’s clear; discussion of diagram.*  *Describe input process output storage boundaries.* | **(14 pts)** |  |  |
| Methodology Methodology and justification (**2**)  Correct Methodology Application (**1**),  Design and Development tools (**2**)  Deliverables and milestones **(2)**  *Examinable bits from ideation*  *Proposal, design, test cases documentation doc*  *Proof of concept- modules*  Gantt Chart that makes sense relative to the project **(1)** | **(8 pts)** |  |  |
| Proposal Presentation Table of Contents and List of Figures **(2)**  Are relevant references provided and formatted correctly? **(2)**  Is there a clear and proper use of language? **(1)**  Effective report structure (chapters and sections) and layout **(2)** | **(6 pts)** |  |  |
| Total Marks | **45** |  |  |

|  |  |  |
| --- | --- | --- |
| Verdict (Please tick) | Accept | Reject |

Comments (**Reasons for Reject/Accept**)