NAALAIYA THIRAN
WEB PHISHING DETECTION
PROJECT DESIGN PHASE-I
PROPOSED SOLUTION

SURYA V

SNEHA S

VAISHNAVI M

YUKESH KUMAR S

DR.S.R.MALATHI

CONTENTS

ABSTRACT

- A web service is one of the most important Internet communications software services. Using fraudulent methods to get personal information is becoming increasingly widespread these days. Phishing website is one of the internet security problems that target human vulnerabilities rather than software vulnerabilities. Phishing is a fraudulent technique that is used over the Internet to manipulate users to extract their personal information such as usernames, passwords, credit cards, bank account information, etc. Nowadays Phishing attacks seem to be increasing. The main reason is the recent cause of the UBER attack. Phishing uses email spoofing as its initial medium for deceptive communication followed by spoofed websites to obtain the initial compromise through an employee's SE (Social Engineering).Many cyber infiltrations are accomplished through phishing attacks where users are tricked into interacting with web pages that appear to be legitimate. Our approach provides similar accuracy to blacklisting and whitelisting, ML (Machine Learning) techniques like detecting URL shortener services, presence of IP address in the URL, presence of Unicode in URL, etc. This project aims to develop these methods of defense utilizing various approaches to categorizing websites and narrow them down to the best machine learning algorithm by comparing the accuracy rate, false positive and false negative rate of each algorithm.

NOVELTY

- Our model uses the power of machine learning to detect phishing sites.
- Python serves as a powerful tool to execute the application with Low false positives, High accuracy.
- Uses the latest techniques that give an efficient and great performance.
- It can easily differentiate the fake and safe URLs. If it’s fake means, a warning message will be intimate to the users.

FEASIBILITY OF IDEAS

- Using data visualization and machine learning algorithm, we safeguard the user's data by detecting malicious websites.
- This application is easy to be built we have a lot of existing software tools that aid us in creatin a web phishing detector.
- Faster, easier and seamless performance can be obtained.

BUSINESS MODEL

- Our model can be used by all people to secure their data from malicious websites.
- It’s an open source tool.

SOCIAL IMPACT

- According to recent research by Google, there was a 3505 increase in phishing websites from January to March 2020.
- Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities.
- As an impact of this model, people can able to find out fraudulent websites or fake ones.
- So that, they can avoid sharing sensitive data with unrecognized websites.

SCALABILITY OF SOLUTION

- This project presents a proposal for scalable detection and isolation of phishing.
- It works on all types of websites and domains.
- It’s possible to make changes to software, which can accept new testing data and should also take part in training data and predict accordingly.
- In future prediction, modules can be improved and integrated.