WEB PHISING DETECTION - PROPOSED SOLUTION

PROBLEM STATEMENT

- Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced.
- Besides, the most common technique used, blacklist-based method is inefficient in responding to emanating phishing attacks since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database.
- Furthermore, page content inspection has been used by some strategies to overcome the false negative problems and complement the vulnerabilities of the stale lists.

IDEA/SOLUTION DESCRIPTION

- **Identify the criteria** that can recognize fake URLs
- **Build a decision tree** that can iterate through the criteria
- **Train our model** to recognize fake vs real URLs
- **Evaluate our model** to see how it performs
- **Check for false positives/negatives**

NOVELTY/UNIQUENESS

- There are three phases in the proposed approach.
- The first stage is the pre-processing stage.
- Through this stage, characteristics and sub-functions are derived from phishing and related websites.

- The second stage contains the classification of machine learning.
- Such classification represents the basis of laws.

- In the third stage, the system classifies the webpages into phishing or normal webpages.
- Semantic features refer to annotations that are derived from the URLs and content of the resources.
- We are motivated to show the value of using semantic features as a means of detecting phishing webpages.

SOCIAL IMPACT/CUSTOMER SATISFACTION

- 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.
- These effects work together to cause loss of company value, sometimes with irreparable repercussions.
- 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.
- These effects work together to cause loss of company value, sometimes with irreparable repercussions.
- To fully understand the impact of phishing attacks on businesses, you would need to get a grasp of the common types of phishing scenarios that exist.

BUSINESS MODEL

- Most people completely overestimate their ability to identify a phishing attack.
- As users, we've been bombarded for years with "phishing" training that has largely been in the form of the "don't click" ideology.
- Phishing is generally defined as a social engineering attack against the end-user and is the primary attack vector for almost every single cyber-attack.
- It is the vehicle that threat actors use to start a breach attempt, how most credential theft occurs, and how most malware is delivered.

SCALABILITY OF THE SOLUTION

- The tremendous and jaw-dropping growth in the deployment of web applications comes hand-in-hand with apprehensions over security.
- Undeniably, the security of web applications has to be addressed at every step of the software development life cycle (SDLC), and even after the deployment of the application is complete.
- To decrease the possibility of latter scenarios, it is important to be cautious of security. On top of that, scaling the application on the basis of unforeseen demand, usage, and traffic is extremely important.