**PROBLEM STATEMENT FOR WEB PHIHSING DETECTION**

**PROBLEM**

Phishing is a common attack on credulous people by making them to disclose their unique information using counterfeit websites. The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions

**BACKGROUND**

Phishing attack has become one of the most serious issues in today's world. Many people have lost huge sums of money by becoming victim to these attacks. Phishing websites trick internet users into divulging their personal or financial information such as username, password, credit card details, bank details etc. These websites look exactly like the original website. Various anti-phishing techniques make use of different features of the webpage in order to identify the fraud website. In this paper, we discuss different phishing detection techniques and present the survey of various phishing website detection approaches

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](https://www.sciencedirect.com/topics/computer-science/phishing-attack)  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. Moreover, page content inspection algorithms each have different approach to [phishing website detection](https://www.sciencedirect.com/topics/computer-science/website-phishing-detection) with varying degrees of accuracy. Therefore, ensemble can be seen to be a better solution as it can combine the similarity in accuracy and different error-detection rate properties in selected algorithms.

**RELEVANCE**

Phishing is a major threat to all Internet users and is difficult to trace or defend against since it does not present itself as obviously malicious in nature. In today's society, everything is put online and the safety of personal credentials is at risk. Phishing can be seen as one of the oldest and easiest ways of stealing information from people and it is used for obtaining a wide range of personal details. It also has a fairly simple approach – send an email, email sends victim to a site, site steals information.

According to Anti-Phishing Working Group (APWG), phishing is a criminal mechanism employing both social engineering and technical tricks to steal user's identity data and financial account credentials by disguising as a trusted one. To lure the end-users, attackers use malicious websites and e-mails by posing themselves as a trusted one. The supreme goal of phishing is to abduct confidential.

data such as user name, password, bank details, credit card details etc. Attackers perform phishing for many reasons – to gain benefits financially, to steal personal information, to ruin the reputation of the organisations and sometimes just to get fame.

**OBJECTIVE**

Phishing aims to collect sensitive and personal information such as usernames, passwords, credit card numbers, and even money by impersonating a legitimate entity in the cyber space.

The main reason is the lack of awareness of users. But security defenders must take precautions to prevent users from confronting these harmful sites. Preventing these huge costs can start with making people conscious in addition to building strong security mechanisms which are able to detect and prevent phishing domains from reaching the user.