Problem statement:

Phishing remains a pervasive and evolving cyber threat that targets users by tricking them into revealing sensitive information through deceptive tactics. Traditional methods to combat phishing, while useful, have limitations, especially as phishing techniques evolve. There is a need for more sophisticated and holistic approaches that incorporate both traditional and advanced techniques, such as machine learning, to effectively mitigate this threat. The rise of online and mobile commerce, driven by advancements in computer networks and cloud technologies, has created opportunities for fraudulent activities, particularly website phishing. This form of cybercrime involves creating fake replicas of legitimate websites to deceive users into revealing sensitive information. Despite various approaches to combat phishing, it remains a persistent threat, causing significant financial damage to individuals, businesses, and governments.

Background of the Problem :

Phishing is a well-known cyber threat that has evolved with the growth of online commerce. Traditional methods to combat phishing, such as user education through training and workshops, have been implemented, but these approaches face challenges like high operational costs and the rapid evolution of phishing tactics. Legal measures have also been introduced to persecute online fraudsters, yet these laws have not been entirely effective in minimizing the severity of phishing. The need for more effective solutions has led to the exploration of intelligent anti-phishing approaches using machine learning technologies. The review highlights the use of machine learning as a promising approach to combat phishing. By integrating classification systems into web browsers, phishing activities can be detected and communicated to users in real-time. However, the effectiveness of this and other approaches varies based on factors such as cost, adaptability, and user experience.

METHOD AND ITS PURPOSE:

This paper reviews and critically analyzes different anti-phishing approaches, including legal measures, user education, and intelligent machine learning technologies. The review compares these approaches by examining their effectiveness, cost, and impact from both the user and performance perspectives. The purpose of the review is to provide a comprehensive understanding of the different strategies available to combat phishing. By highlighting the differences, similarities, and positive and negative aspects of each approach, the review aims to

inform stakeholders, including computer security experts, web security researchers, and business owners, about the most effective ways to mitigate phishing threats.

RESULT:

The review identifies the strengths and weaknesses of various anti-phishing strategies. Traditional methods like user education are not cost-effective due to the changing nature of phishing tactics and the high operational costs involved. Legal approaches, while necessary, have not significantly reduced the threat. Machine learning technologies offer a more promising solution by enabling real-time detection and response to phishing attempts. However, even these advanced techniques must be continuously updated to keep pace with evolving phishing strategies. One major challenge is the high cost and complexity of implementing and maintaining effective anti-phishing measures. Additionally, while machine learning-based systems improve detection, they require ongoing refinement and user education to ensure optimal performance and acceptance.

CONCLUSION:

The paper concludes that combating phishing requires a multifaceted approach. Relying solely on legal measures or user education is insufficient due to the dynamic and evolving nature of phishing tactics. The integration of machine learning technologies into anti-phishing strategies offers a more effective solution, but these must be complemented by continuous education and legal enforcement. The review advocates for a combined approach that includes the use of intelligent technologies, regular user training, and robust legal frameworks to effectively mitigate the risks associated with phishing. Collaboration among stakeholders, including security experts, researchers, and business owners, is essential to developing and implementing comprehensive anti-phishing strategies.