TEAM ID	PNT2022TMID43653
PROJECT NAME	Web Phishing Detection

PROJECT OBJECTIVES

Web phishing is just one of the many security risks that web services face. Phishing assaults are usually detected by experienced users however, security is a primary concern for system users who are unaware of such situations. Phishing is the act of portraying malicious web runners as genuine web runners to obtain sensitive information from the end-user. Phishing is currently regarded as one of the most dangerous threats to web security. Vicious Web sites significantly encourage Internet criminal activity and inhibit the growth of Web services. As a result, there has been a tremendous push to build a comprehensive solution to prevent users from accessing such websites.

Our technology merely examines the Uniform Resource Locator (URL) itself, not the content of Web pages, A protocol used to access the page the server who hosts the web page. A Host name consists of a subdomain name and a domain name. The attacker can register any domain name that has not been registeredbefore. This part of URL can be set only once. The phisher can change Free URL at any time to create a new URL. The reason security defenders struggle to detect phishing domains is because of the unique part of the website domain (the Free URL). When a domain detected as a fraudulent, it is easy to prevent this domain before a user access to it.