Project name	Web phishing detection
Team id	PNT2022TMID43023

OBJECTIVES OF THE WEB PHISHING DETECTION

- Phishing is the fraudulent attempt to steal the private information's for malicious use . Such as , login credentials or account information by sending as a reputable entity of a persons email or other communication channel . Phishing attacks are occur in various sector but , it is mostly targeted in online sector and webmail .
- Typically a victim receives a massage as appear to have been sent by a known person or any organization. A massage contains malicious software to targeting . The users computer or their links to direct victims to malicious websites in order to trick them into divulging personal and financial information , such as username , passwords , credit card details by way of impersonating a legitimate entity.
- Phishing is a popular cybercrime of today use , since it is easier to trick someone into click a malicious link . Which seems legitimate then trying to break through a computers defence systems and property damage .
- A protocol use to access the page and the server who host the web page . A host name consists of sub domain name .the attackers register any domain name that has not been register before .
- 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. Because of the unique part of the website domain(the free URL) . When a domain easier to detected a fraudulent attempts . It is easy to prevent this domain before an user access to it .