Model Development Phase Template

Date	10 june 2024
Team ID	739879
Project Title	Detection of phishing websites from URLs
Maximum Marks	5 Marks

Feature Selection Report Template

In the forthcoming update, each feature will be accompanied by a brief description. Users will indicate whether it's selected or not, providing reasoning for their decision. This process will streamline decision-making and enhance transparency in feature selection.

Feature	Description	Selected (Yes/No)	Reasoning
Having_iphaving_ip_address	The unique identifying number assigned to every device connected to the internet	yes	For predicting the phishing websites, a having ip address is required
URLURLlenth	url length measure the number of character that a url consist of.	Yes	They contain additional characters to evade detection or deceive users.
Shortining service	Generate shorter aliases for long URLs	Yes	To conceal the original URL, making it difficult to identify the destination website, which is a common tactic used by phisher to trick users into clicking on malicious links

Having at symbol	Used to direct electronic communication to specified entities, most notably in email addresses and social media handles	Yes	The reason for having an “@” symbol in a URL is often a tactic used by phisher to trick users into thinking the URL is legitimate, as the “@” symbol can be used to hide the actual domain name and make the URL appear more authentic.

Double slash redirecting	Effectively at the start of the URL path you would normally define in your application when constricting internal anchors/URLs	Yes	Phisher use is to trick use it to trick users into thinking they are on a legitimate website, as the double slash can be used to redirect to different domain or websites, potentially leading to a phishing websites
Prefix suffix	Checking for the presence of “-“ in the URL’s domain part	Yes	Phisher often add extra characters or words to the beginning or end of the legitimate domain name to create a similar -looking URL, attempting to trick users into thinking it’s the real website
Having sub domain	It may indicate a phishing attempt	Yes	In URL is that phisher often use subdomains to create a URL that appears to be from a legitimate domain, but actually leads to a phishing page, making it harder for users to identify the scam
SSL final start	The presence of “https” and “ssl” are indicates legitimate site	Yes	Having a valid SSL certificate at the start of a URL indicates that the website is taking steps to protect user data and ensure a secure browsing experince
Domain registration length	Domain registration length refers to the duration of time a domain name has been registered .	Yes	By considering domain registration length, phishing detection systems can identify potentially suspicious domain and take appropriate action to protect users.

favicon	Credit history of the applicant	Yes	A major factor in loan approval is reflecting the applicant's creditworthiness.
status	Identify phishing or legitimate	Yes	The target variable for predictive modeling – is essential for the project's goal.