PROBLEM STATEMENT

The main purpose of the project is to detect the fake or phishing websites who are trying to get access to the sensitive data or by creating the fake websites and trying to get access of the user personal credentials

Whom does the problem affect?	*Many users and organizations have fallen victim to phishing attacks, whereby their personally identifiable information, credentials and sensitive data have been stolen, resulting in identity theft, loss of money, loss of reputation, loss of intellectual property, as well as disruption of daily normal operational activities.*
What are the boundaries of the problem?	*Phishers start by configuring a fake website of a targeted victim brand before deploying publicly with a phishing URL. Then, the phisher launches a campaign to distribute the phishing URL through emails, instant messages, or text messages. Some victim users start visiting the fake website and few provide their sensitive information.*
What is the issue?	*Malicious links will lead to a website that often steals login credentials or financial information like credit card numbers.*

When does the issue occurs?	*The issue occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.*
Where is the issue occurring?	*96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone.*
Why is it important that we fix the problem?	*With the sensitive information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in your name. They can do damage to your financial history and personal reputation that can take years to unravel.*