

WEB PHISHING DETECTION

DOMAIN: Data science.

PROBLEM STATEMENT:

- 1) Phishing Web Websites are duplicate pages created to mimic real Websites in-order to deceive people to get their personal information.
- 2) Because of the adaptability of their tactics with little cost Detecting and identifying Phishing Websites is really a complex and dynamic problem.
- 3) There are a number of users who purchase products online and make payments through e-banking.
- 4) There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons.
- 5) This type of e-banking website is known as a phishing website.
- 6) Web service is one of the key communications software services for the Internet.
- 7) Web phishing is one of many security threats to web services on the Internet.

COMMON THREATS OF WEB PHISHING:

- 1) Phishing. Phishing attacks involve attackers targeting users through email, text messages, or social media messaging...
- 2) Ransomware. Ransomware is a form of malware that results in an attacker holding their victim's data or computer hostage.
- 3) SQL Injection. Structured Query Language (SQL) is a computing language used to search and query databases. SQL injection.
- 4) Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity.
- 5) It will lead to information disclosure and property damage.

6) Large organizations may get trapped in different kinds of scams.

This Guided Project mainly focuses on applying a machine-learning algorithm to detect phishing websites.

In order to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. We implemented classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy. The e-banking phishing website can be detected based on some important characteristics like URL and domain identity, and security and encryption criteria in the final phishing detection rate. Once a user makes a transaction online when he makes payment through an e-banking website our system will use a data mining algorithm to detect whether the e-banking website is a phishing website or not.

MODEL FOR WEB PHISHING DETECTION:

