Web Phishing Detection

In phishing, attackers lure end-users and steal their personal information. To minimize the damage caused by phishing must be detected as early as possible. There arevarious phishing attacks like spear phishing, whaling, vishing, smishing, pharming and so on. There arevarious phishing detection techniques based on whitelist, black-list, content-based, URL-based, visual similarity and machine-learning. In recent years, advancements in Internet and cloud technologies have led to a significant increase in electronic trading in which consumers make online purchases and transactions. This growth leads to unauthorized access to users' sensitive information and damages the resources of an enterprise. Phishing is one of the familiar attacks that trick users to access malicious content and gain their information.

- Money stolen from bank accounts
- Loans and mortgages opened in a person's name
- Lost access to photos, videos, files, and other important documents
- Fake social media posts made on a person's accounts
- Exposed personal information of customers and co-workers
- Outsiders can access confidential communications, files, and systems
- Files become locked and inaccessible

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

In order to detect and predict phishing websites, we propose an intelligent, flexible and effective system that is based on using classification algorithms. The phishing website can be detected based on some important characteristics like URL and domain identity, and security encryption criteria. Once a user provides his sensitive information our system will use a data mining algorithm to detect whether the website is a phishing website or not.