**WEB PHISING DETECTION**

**PROJECT OBJECTIVE:**

**WEB PHISING:**

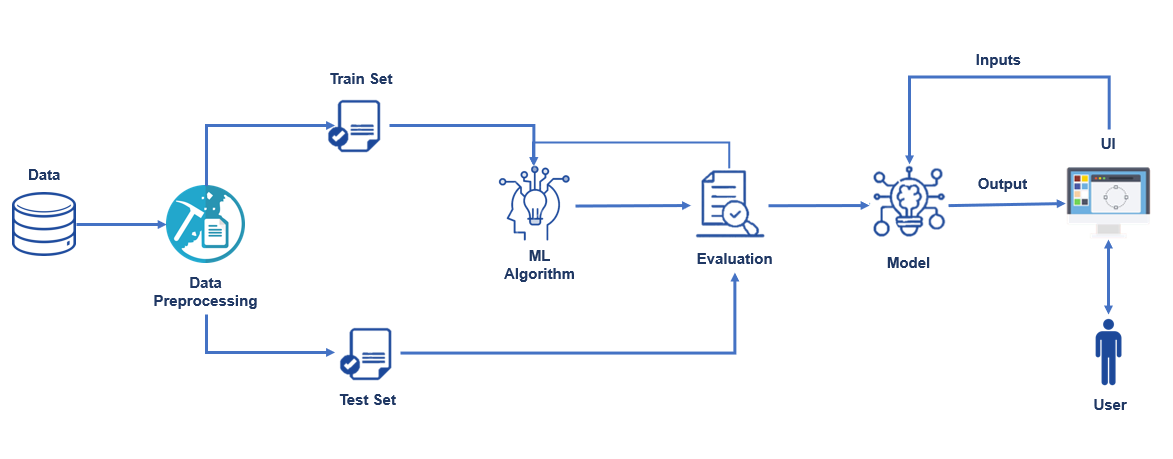
* Web Phishing is a type of Social Engineering attack in which the victims are psychologically manipulated to provide sensitive information or install malicious programs.
* In Phishing the cyber attackers use fake offers, warnings as bait to trap users into their scam.
* The attackers can perform Phishing through emails, SMS, phone call, fake websites, and even face to face.

**DANGER IN WEB PHISHING:**

* Infect the device with malware.
* Steal the private credentials to get your money or identity.
* Obtain control of your online accounts.
* Convince you to willingly send money or valuables.

**TYPES OF PHISING ATTACKS**:

* + **Phishing email**:
    - It appears in email inbox, usually with a request to follow a link, send a payment, reply with private info, or open an attachment.
  + **Domain spoofing:**
    - **It** is a popular way an email phisher might mimic valid email addresses. These scams take a real company’s domain (ex: @america.com) and modify it.
  + [**Voice phishing (vishing)**](https://www.kaspersky.com/resource-center/definitions/vishing):
    - scammers call you and impersonate a valid person or company to deceive you. They might redirect you from an automated message and mask their phone number.
  + **SMS phishing (smishing):**
    - It is similar to vishing, this scheme will imitate a valid organization, using urgency in a short text message to fool you.
  + **Social media phishing**:
    - It involves criminals using posts or direct messages to persuade you into a trap.
  + **Clone phishing**:
    - It duplicates a real message that was sent previously, with legitimate attachments and links replaced with malicious ones.

**ARCHITECTURE FOR WEB PHISING DETECTION:**

**FEATURES OF WEB PHISING DETECTION:**

1. URL-Based Features
2. Domain-Based Features
3. Page-Based Features
4. Content-Based Feature

**URL-Based Features**

URL is the first thing to analyse a website to decide whether it is a phishing or not. Some of URL-Based Features are given below.

* Digit count in the URL
* Total length of URL
* Checking whether the URL is Typo squatted or not. (google.com → goggle.com)
* Checking whether it includes a legitimate brand name or not (apple-icloud-login.com)

## Domain-Based Features

The purpose of Phishing Domain Detection is detecting phishing domain names.

## Page-Based Features

Page-Based Features are using information about pages which are calculated reputation ranking services. It involves:

* Global Page rank
* Country Page rank

**Content-Based Features**

Page contents are processed for us to detect whether target domain is used for phishing or not. Some processed information about pages are given below.

* Page Titles
* Meta Tags
* Hidden Text