Project name - spam/ phishing detector system

Team name - identifiers

Member name-
Name : NItesh Shedge
roll no :47
Mail- niteshshedge011@gmail.com

Name : Dishant chikhale
roll no :06
Mail- dishantchikhale1405@gmail.com

The purpose of a spam message detection system is to identify and filter out unwanted, unsolicited, or harmful messages—typically in emails, SMS, or online platforms—to protect users and systems from:

Junk content that clutters inboxes or feeds.

Phishing attempts aimed at stealing sensitive information.

Malware distribution through links or attachments.

Scams and frauds such as fake offers or lottery messages.

Resource misuse like overloading servers or wasting bandwidth

Importance :

Security: Spam often contains phishing links, malware, or other harmful content that can compromise personal data, systems, or entire network

Protects Reputation

For businesses and service providers: Allowing spam to reach users can damage the credibility and trustworthiness of a service or platform.

Productivity: Filtering out spam helps users and organizations avoid wasting time sorting through irrelevant or malicious messages

User Experience: A clean inbox improves usability and helps users focus on legitimate and important communications.

How it works

Spam messages work by exploiting communication systems—like email, SMS, social media, or messaging apps—to send unwanted, unsolicited messages to a large number of recipients. Here's how they typically operate:

Message Collection and Targeting

Harvesting contacts: Spammers use bots, data breaches, or buy lists to collect large numbers of email addresses or phone numbers.

Targeting: Some spam is random, while others are tailored using stolen personal info (called spear-phishing).

Message Generation

Automation tools: Spammers use scripts or spam-sending software to create and send messages in bulk.

Content: Messages often include:

Ads or affiliate links for products/services.

Scams (e.g., "You've won!" or fake investment offers).

Phishing links to steal personal or financial information.

Malware attachments or links to infected websites.

Earning of spamers

Sending the Messages

Botnets: Networks of infected computers (bots) send spam on behalf of the spammer to avoid detection.

Compromised accounts: Sometimes real email or social accounts are hijacked to bypass spam filters.

Obfuscation: Spammers use tactics like URL shorteners, misspelled words, or invisible text to trick spam filters

Monetization

Spammers earn money by:

Ad revenue: Driving traffic to sites filled with ads.

Affiliate marketing: Getting paid per click or sale from links.

Fraud: Tricking victims into paying money or giving up sensitive information.

How our website works

It verifies the messages and link which is send by anyone else. Suppose if someone who is not in your contact list has sent you any message or link you just have to copy it and paste it on our websites it shows you the result that the message or link is how much safe . Like it gives you the number of percentage that how the link or message is safe. It helps you to identity the safety of the link or message of it is not safe it can harm your device, it can hack your device and can leake your personal information,photos, videos or any other important things. It can become a very helpful for the clients in case of detecting spam messages which plays a very important role in every person's day to day life.

YouTube link of demonstration

https://youtu.be/b3OJJ-JsSzI?si=LSnrrIFumEZswtXa