WEB PHISHING DETECTION

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

Duplicate websites are easily created

Gaining credentials is the objective of the hacker

Phishing attacks are advanced nowadays

What do they THINK AND FEEL?
what really counts
major preoccupations
worries & aspirations

Similarities in malicious URLs

Check whether the sender's address is legitimate

What do they HEAR?
what friends say
what boss say
what influencers say

Poor grammar and spellig are also red flags

Requests for personal information are red flags

Be cautious of links recieved

Will the project be able to detect all malicious URLs?

What algorithm is used to detect these attacks?

What do they SEE?
environment
friends
what the market offers

Customer information is protected

What do they SAY AND DO?
attitude in public
appearance
behavior towards others

Cyber attacks are prevented

Increases awareness of such attacks

User is vulnerable to further attacks

Loss of privacy

Personal information stolen

PAIN
fears
frustrations
obstacles

Damage of reputation for the organisation

Provides more security

GAIN
"wants" / needs
measures of success
obstacles

Benefits both organization and customer

Makes online transactions more secure