WEB PHISHING DETECTION

THINK & FEEL

- To Catagorize and Classify the vulnerability issues in Internet Computing Security
- To make the analysis of vulnerability issues and recover The vulnerabilities
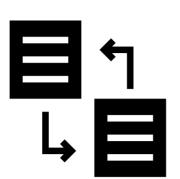- Prevent A organization's upcoming projects and Employee's data from leaking.
- confirm whether the website link send by any person which is safe or not
- Main objective is to avoid installation of Malware
- To avoid The leakage of our personal details and bank account details

HEAR

- E-MAIL phishing Spear phishing Clone Phishing Popup Phishing Whaling phishing
- Infect your device with Malware and access your datas
- Steal your private credentials to get your money or identity
- Obtain control of your online accounts
- Convince you to willingly send money or valuables

SEE

- List Based Detection
- Machine Learning-Based Detection
- Hybrid Methods
- Heuristic-Based Detection
- Deep Learning Detection

SAY & DO

- By Providing Anti phishing training
- Ensure compliance and Reassure insurers
- Ensure end to end security
- Never trust alarming messages
- Review account statements regularly
- Limit User acess to high- value systems and data
- Dont give your information to an unsecured site

PAINS

- Phishing is difficult because scams ae nothing new on internet
- Inability to detect phishing website
- Steal intellectual property
- Damage to reputation

GAINS

- Eliminate the cyber threat risk level
- Prevents unauthorised spoofing
- Build Secure connection
- Deploy targeted anti-phishing solution