What are the thoughts about this project?	What is the purpose?
- Phishing offenses are increasing, resulting in billions of dollars in loss - The Software-as-a-Service (SaaS) and webmail sites are the most common targets of phishing - - Attackers can steal the victims private info and can also spread other types of malware	- Experts can identify fake websites but not all the users can identify the fake website and such users become the victim of phishing attack - To create user awareness about phishing attacks

WEB PHISHING DETECTION

What are the existing solutions?	What is the proposed solution?
- Techniques based on blacklists/whitelists - Techniques based on natural language processing - Techniques based on visual similarity - Techniques based on rules of URL	- Machine learning based techniques wher a classification model is trained using various heuristic features - Heuristic features are URL, webpage content, website traffic, search engine, WHOIS record, and Page Rank

PAIN	GAIN
- The heuristic features are not warranted to present in all phishing websites and might also present in the benign websites, which may cause a classification error - Some of the heuristic features are hard to access and third-party dependent - Services may inaccurately identify the new benign website as a phishing site due to the lack of domain age	- Real-time detection - High detection efficiency - Target independent - Third-party independent - Light-weight technique