WEB PHISHING DETECTION

1. Team Leader - KESHAV KHANTH T
2. Team Member 1 - HARISH R
3. Team Member 2 - LOKESH SUNIL D
4. Team Member 3 - SARATH KUMAR I

ABSTRACT

- Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels. Phishing attacks can paralyze a business. Staff might be unable to continue their work. Data and assets might be stolen or damaged. Customers might be unable to access online services.
- The reason security defenders struggle to detect phishing domains is because of the unique part of the website domain. Social Impact. It will help to minimize the frauds while using software solutions (EX: Web applications, etc).
- In conclusion, this system is designed for resources are used as intended, prevents from valuable information from leaks out, produce better control mechanism and alerts the user to keep their private information safe.

EXISTING SOLUTION:

- https://checkphish.ai/

REFERENCES:

- https://towardsdatascience.com/phishing-domain-detection-with-ml-5be9c99293e5
- https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-net.2020.0078

LITERATURE SURVEY

S.NO	TITLE OF JOURNAL	AUTHOR	YEAR OF PUBLICATION	INFERENCES	PROS & CONS
1.	“A Framework for Auto-Detection of Phishing Websites”	Hossein Shirazi, Kyle Haefnar, Indrakshi Ray.	2017	For phishing websites, machine-learning data can be created using this framework. In this, they have used reduced features set and using python for building query. They build a large labeled dataset and analyze several machine-learning classifiers against this dataset	Analysis of this gives very good accuracy using machine-learning classifiers. These analyses how long it takes to train the model.
2.	"Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms"	Longfei Wu etal..., "	2016	In this paper, author did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including the web page	Existing schemes designed for web phishing attacks on PCs cannot effectively address the

				phishing attacks.	various phishing attacks on mobile devices. It verifies the validity of web pages, applications, and persistent accounts by comparing thee actual Identity to the claimed identity
3.	"A Literature Survey on Social Engineering Attacks: Phishing Attacks," in International Conference on Computing, Communication and Automation”	Surbhi Gupta etal., "A	2006	To fool an online user into elicit personal Information. The prime objective of this review is to do literature survey on social engineering attack: Phishing attacks and techniques to detect attack.	The paper discusses various types of Phishing attacks such as Tab-napping, spoofing emails, Trojan horse, hacking and how to prevent them.
4.	“A Hybrid Model to Detect		2016	In this paper, a proposed	They achieved

	Phishing-Sites using Supervised Learning Algorithms”			model was carried out in two phases. In phase 1 individually perform classification techniques, and select the best three models. In phase 2, they further combined each individual model with the best three models and made a hybrid model that gives better accuracy than individual models.	97.75% accuracy on the testing dataset. There is limitation of this model that it requires more time to build hybrid model
5.	“Phishing : An Analysis of a Growing Problem"	SANS Institute, "	2017	This paper gives an in depth analysis of phishing: what it is the technologies and security Weaknesses it takes advantage of the dangers it poses to end users.	In this analysis author explain the concepts and technology behind phishing, show how the threat is much more then just a nuisance or passing trend, and discuss

					how gangs of criminals are using.
6.	“Detecting phishing using machine learning IEEE Conference publication |” IEEE Explore	Mohammed Hazim Alkawaz	2020	Anomaly detection solutions are readily available, are deployed quickly and immediately and automatically protect all account holders against all types of fraud attack with minimal Disruption to legitimate online banking activity	Limitation of this project is there was no facility of displaying pop-up and email notification once user had access blacklisted website
7.	“Detection of phishing websites using an efficient feature-based machine learning framework”.	Naresh Kumar, Premnath , Nishanth Kumar V, Nemala Sai Rama Hemnah.	2018	In this, they have classified extracted features into three categories such as URL Obfuscation features, Third-Party-based features, Hyperlink-based features.	Moreover, the proposed technique gives 99.55% accuracy. Drawback of this is that as this model uses third party features, classification of websites depends on the speed of third-party services.