BIBLIOGRAPHY

1. D. R. Patil, J. B. Patil, “Survey on Malicious Web Pages Detection Techniques, Science and Technology”, 2015 International Journal of u and e Service.

2. B. Wardman, G. Shukla and G. Warner,” Identifying vulnerable websites by analysis of common strings in phishing URLs,”; 2009 eCrimeResearchers Summit, Tacoma, WA, 2009,

3. A. B. Sayambar, A. M. Dixit, “On URL Classification, International Journal of Computer Trends and Technology” 2014.

4. Xiang et al., “A Feature-Rich Machine Learning Framework for Detecting Phishing WebSites, ACM Transactions on Information and System Security “2011.

5. A. Abunadi, O. Akanbi and A. Zainal,” Feature extraction process: A phishing detection approach,” 2013 13th International Conference on Intellient Systems Design and Applications, Bangi, 2013,

6. M. Aydin and N. Baykal,” Feature extraction and classification phishing websites based on URL,” Communications and Network Security (CNS), 2015 IEEE Conference on, Florence, 2015

7. Abu-Nimeh S., Nappa D., Wang X., & Nair S. (2007).” A Comparison of Machine Learning Techniques for Phishing Detection”. APWG eCrimes Researchers Summit

8. James, Joby, L. Sandhya, and Ciza Thomas,” Detection of phishing URLs using machine learning techniques,” Control Communication and Computing (ICCC), 2013 International Conference on. IEEE, 2013.

9. Hou et al., “Malicious Web Content Detection by Machine learning, Expert Systems with Applications”, International Journal 2010.

10. G. Venkataraman and A. Ravichandran,” Adaptive Semantic Search: Re-Ranking of Search Results Based on Webpage Feature Extraction and Implicitly Learned Knowledge of User Interests,” Semantics, Knowledge and Grids (SKG), 2014 10th International Conference on, Beijing, 2014.

11. Khamis et al, “Characterizing A Malicious Web Page”, Australian Journal of Basic and Applied Sciences 2014.

12. Curtsinger et al., “Zozzle: Fast and Precise In-Browser JavaScript Mal- ware Detection”, SEC’11 Proceedings of the 20th USENIX conference on Security 2011.

13. Zhou et al., “Malicious Websites Detection and Search Engine Protection”, Journal of Advances in Computer Network 2013.

14. M. Aldwairi, R. Alsalman MALURLS: “A Lightweight Malicious Website Classification based on URL features, Web Intelligence”, 2012 Journal of Emerging Technologies.
15. Eshete et al., Malicious Website Detection: Effectiveness and Efficiency Issues, SysSec Workshop (SysSec) 2011.
16.” UCI Machine Learning Repository: DataSet”, Archive.ics.uci.edu, 2017. [Online]. Available: http://archive.ics.uci.edu/ml/datasets/Phishing+Websites UCI Phishing Websites Data Set.
17. Ma et al., Beyond Blacklists:” Learning to Detect Malicious Web Sites from Suspicious URLs, Knowledge discovery and data mining”, 2009 15th ACM SIGKDD international conference.
18. Canali et al., Prophiler: “A Fast Filter for the Large-Scale Detection of Malicious Web Pages”, Web Security, 2011, WWW’11.
19. Choi et al., “Detecting Malicious Web Links and Identifying their attack types, Web application development”, 2011 2nd USENIXconference.
20.” What are extensions? - Google Chrome”, Developer.chrome.com, 2017. [Online]. Available: https://developer.chrome.com/extensions.
21. J. Brownlee,” Tutorial to Implement k-Nearest Neighbors in Python from Scratch - Machine Learning Mastery”, Machine Learning Mastery. [Online]. Available: http://machinelearningmastery.com/tutorial-to-implement-k-nearest-neighbors-in-python-from-scratch/.
22. J. Brownlee,” Support Vector Machines for Machine Learning - Machine Learning Mastery”, Machine Learning Mastery, 2017. [Online]. Available: http://machinelearningmastery.com/support-vector-machines-for-machine-learning/.
23.” Random Forests Algorithm”, Datasciencecentral.com, 2017. [Online]. Available: http://www.datasciencecentral.com/profiles/blogs/random-forests-algorithm.
24.” Light Gradient Boost”, LGBM, [Online]. Available: https://lightgbm.readthedocs.io/en/latest/
25.” Artificial Neural Network”, Keras Documentation, [Online]. Available: https://keras.io/