IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

Prediction of Phishing using Machine Learning

Sivalakshmi S[1], Vichitra Devi M[2], Kalpana R[3], Dr. M. Preetha[4]
Students, Department of Information Technology[1,2]
Professor, Department of Information Technology[3]
Head of Department, Department of Information Technology[4]
Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India

Abstract: *Phishing is a common attack on credulous people by making them to disclose their unique information using counterfeit websites. The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions. Phishes use the websites which are visually and semantically similar to those real websites. As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing. Machine learning is a powerful tool used to strive against phishing attacks. Phishing is popular among attackers, since it is easier to trick someone into clicking a malicious link which seems legitimate than trying to break through a computer's defense systems. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization using that organization's logos and other legitimate contents. Here, we explain phishing domain (or Fraudulent Domain) characteristics, the features that distinguish them from legitimate domains, why it is important to detect these domains, and how they can be detected using machine learning and natural language processing techniques. In this paper, we compared the results of multiple machine learning methods for predicting phishing websites.*

Keywords: Phishing, Personal information, Machine Learning, Malicious links, Phishing domain characteristics

REFERENCES

[1]. Desai, J. Jatakia, R. Naik, and N. Raul, "Malicious web content detection using machine leaning," RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc., vol. 2018–Janua, pp. 1432–1436, 2018.

[2]. P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta, "Phish Net: Predictive Blacklisting to Detect Phishing Attacks," 2010.

[3]. Bradley Barth, "SOC teams spend nearly a quarter of their day handling suspicious emails,"https://www.scmagazine.com/home/email-security/soc-teams-spend-nearly-a-quarter-of-their-day-handling-suspicious-emails. 2021.

[4]. Crane Hassold, "Employee-Reported Phishing Attacks Climb 65%, Clobbering SOC Teams," https://www.agari.com/email-security-blog/employee-reported-phishing-attacks-soc/. 2020.

[5]. A. Y. Fu, W. Liu, and X. Deng, "Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD)," IEEE Trans. Dependable Secur. Comput, vol. 3, no.4, pp. 301–311, 2006, doi: 10.1109/TDSC.2006.50.

[6]. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural Markers of Cyber security: An fMRI Study of Phishing and Malware Warnings," IEEE Trans. Inf. Forensics Secur., vol. 11, no.9,pp. 1970–1983, 2016, doi: 10.1109/TIFS.2016.2566265.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 8, May 2022
Impact Factor: 6.252

[7]. X. Zhang, Y. Zeng, X. Jin, Z. Yan, and G. Geng, "Boosting the Phishing Detection Performance by Semantic Analysis," 2017.

[8]. L. MacHado and J. Gadge, "Phishing Sites Detection Based on C4.5 Decision Tree Algorithm," in 2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017, 2018, pp. 1–5.

[9]. A. Desai, J. Jatakia, R. Naik, and N. Raul, "Malicious web content detection using machine leaning," RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc., vol. 2018–Janua, pp. 1432–1436, 2018.

[10]. https://www.researchgate.net/publication/355263255_Detecting_phishing_websites_using_machine_learning_technique