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

A Study on Various Phishing Techniques and Recent Phishing Attacks

Bhagya Bajanthri[1] and Mr. Sayeesh[2]
Student, Department of Computer Science and Engineering[1]
Assistant Professor, Department of Computer Science and Engineering[2]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *Now-a-days internet has become a very unsafe space to deal with. Hackers are constantly trying to gain the user's personal information, and detailed credentials. So many websites on the internet, even though safe, this safety cannot be assured by all websites. These rule breakers avoid abiding by rules, and try to employ methods like trickery and hacking to gain illegal access to private information. To be able to overcome this problem, we need to first understand the intricacies of how the virus is designed. This paper mainly deals with the different phishing techniques and recent phishing attacks that took place during COVID 19. like Link Manipulation, Filter Evasion, Website Forgery, Phone Phishing and Website Forgery. We have also studied a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attackers website called Convert Redirect. In this paper, we present some phishing examples like Paypal phishing which involves sending an email that fraudulently claims to be from a well known company and Rapidshare Phishing where in the spoofed web page, phishers attempt to confuse their victims just enough to entice them to enter their login name and password. To perform these types of phishing the Phishers uses so many phishing techniques like Link Manipulation, Filter Evasion, Website Forgery, Phone Phishing and Website Forgery. Phishing techniques include the domain of email messages. Phishing emails have hosted such a phishing website, where a click on the URL or the malware code as executing some actions to perform is socially engineered messages. Lexically analyzing the URLs can enhance the performance and help to differentiate between the original email and the phishing URL. As assessed in this study, in addition to textual analysis of phishing URL, email classification is successful and results in a highly precise anti phishing. From the thorough analysis of the research paper, we have understood how phishing attacks work and the different methods employed to carry out the attack. Also, we have studied some of the most recent phishing attacks and measures taken by the authorities to overcome and prevent any such attacks in future.*

Keywords: Phishing Attacks.

REFERENCES

[1] For phishing email," J.Comput. Secur., vol. 18, pp. 7-35, January 2010. [Online]. Available:http://portal.acm. org/citation.cfm?id=17 34234.1734239
[2] http://www.hackersonlineclub.com/tab-nappinu
[3] krebsonsccurity.com
[4] www.tripwirc.com/
[5] http:/ /en. wikipedia.org/
[6] http://webopedia.com/
[7] http://computcrworld.com/
[8] A.-P. W. G. (APWG), "Phishing activity trends report", 2009, [online] Available: http://wwwantiphishing.org/ reports/apwgreport Q32009.pdf.
[9] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong and C. Zhang, "An empirical analysis of phishing blacklists", 2009, [online] Available: http://ceas.cc/2009/papers/ceas2009-paper-32

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

[10] Fette, N. Sadeh and A. Tomasic, "Learning to detect phishing emails", Proceedings of the 16th international conference on World Wide Web ser. WWW '07, pp. 649-656, 2007.

[11] A Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paafi and S. Strobel, "New filtering approaches for phishing email", J. Comput. Secur., vol. 18, pp. 7-35, January 2010.

[12] "International Journal Of Scientific & Technology Research", 90 ijstr©2012, vol. 1, no. 6, July 2012, ISSN 2277-8616.