iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51502

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Anti-Phishing Tools: A Thorough Comparison of Features and Performance

Ishant Sharma[1], Aman Kumar Sharma[2]
[1,2]*Himachal Pradesh University, Shimla, Himachal Pradesh, India*

***Abstract*: Phishing attacks are a common form of cyber-attacks that can result in data breaches, financial losses, and harm an organization's reputation. The purpose of the study is to evaluate and compare three popular anti-phishing tools' effectiveness in detecting and preventing such attacks. The research method involves conducting a study to identify best performing anti-phishing tool. The findings show that some tools have high accuracy; others have a lower false positive rate.**
Overall, this research paper provides useful information about the effectiveness of anti-phishing tools and can help organizations select the most appropriate tool for their specific needs.
Keywords: Phishing, Anti-Phishing Tools, True Positive Rate, False Positive Rate, Accuracy, Database.

I. INTRODUCTION

Phishing attacks have emerged as a severe threat to organizations worldwide, causing substantial financial losses, reputational damage, and data breaches.
The utilization of anti-phishing tools has become increasingly prevalent to detect and prevent these attacks. Given the plethora of anti-phishing tools available in the market, choosing the appropriate tool capable of accurately identifying and mitigating phishing attacks is critical. [1]
The Anti-Phishing Working Group (APWG) in their report in Q2 of 2019 said that webmail and software as a service (SaaS) are the most targeted industries in phishing. [2][3]
According to Phishlab's phishing report in 2019, financial services, shipping, payment services and cloud storage services are target of 84% of the phishing attacks. [2][4]
This research paper aims to provide a comprehensive comparison of three popular anti-phishing tools based on their accuracy in detecting and preventing phishing attacks. The evaluation will encompass various parameters, including accuracy, true positive rate, false positive rate and ease of use.
The study's findings will equip organizations with an understanding of the differences between anti-phishing tools and enable them to select the most suitable tool that aligns with their specific needs. The study will also emphasize the importance of employing multiple anti-phishing tools to provide comprehensive protection against phishing attacks. This research paper contributes to the development of effective cyber security strategies that can safeguard organizations against the escalating threat of phishing attacks.
Section II of this paper explains phishing taxonomy. Section III tells about the tools used, their history and features. Section IV is about the analysis of the tools and result after testing the tools. Section V is conclusions and future scope of this research.

II. PHISHING TAXONOMY

There are several phishing taxonomies, including:

A. Email Phishing

This is the most frequently encountered form of phishing attack, in which an attacker sends a fraudulent email that appears to be from a legitimate entity, such as a bank, social media network, or a reputable company. The email mostly contains a link that leads the victim to a fake website that is intended to pilfer their private information [1]. According to a research of Ironscales in 2021, it was found that after March 2021 81% organizations worldwide experienced increase in email phishing attacks. [5]

B. Spear Phishing

A particular person or organization is target of this type of attack, often using personal information that has been gathered from social media or other sources. The attacker may use this information to create a more convincing email or website that is tailored to the victim's interests or job role. [6]

©IJRASET: All Rights are Reserved

C. Smishing

In this form of phishing attack SMS text messages are used to trick victims into clicking on a link or providing personal information. The messages often appear to be from a legitimate source, such as a bank or social media platform [7]. According to a research conducted by FBI's Internet Crime Complaint Centre in 2021, it was found that smishing and vishing is the most common threat in the US with 323,972 victims. [8]

D. Vishing

This is a type of phishing attack that leverages voice calls to deceive victims into divulging personal information. The attacker may employ social engineering tactics to coerce the victim into disclosing confidential data or executing a specific task. [1]

E. Clone Phishing

This type of attack involves creating exact replica of a legitimate email or website, and then replacing it with a fraudulent one. The attacker may do this by copying the original content and then making small changes, such as altering the link or adding a malicious attachment. [9]

F. Whaling

This is a kind of phishing attack aimed at senior executives or individuals possessing confidential data. The attacker might employ social engineering methods to generate a feeling of haste or compulsion in the target to furnish the data. [9]

G. Malware-Based Phishing

This type of attack involves sending an email or message that contains malware, such as a virus or Trojan horse. By clicking on a link or opening an attachment, the victim could be deceived into downloading the malware. [10]

H. Search Engine Phishing

This type of attack requires creating fraudulent websites that are originated to appear at the top of search engine results. The attacker may use black hat SEO techniques to trick search engines into ranking their website higher, and then direct users to the fake website to steal their personal information.[11][12]

I. Man-in-the Middle (MITM) Phishing

This type of attack involves intercepting communication between the victim and a legitimate website or service, and then using a fake website or service to steal their personal information. The attacker may use techniques such as session hijacking or DNS spoofing to redirect the victim to the fake website. [10][12]

J. Content Injection Phishing

This type of attack involves injecting malicious content into a legitimate website or service, in order to trick the victim into providing their personal information. For example, the attacker may create a fake login page that appears to be part of a legitimate website, but actually captures the victim's username and password.[11][12]

III. ANTI PHISHING TOOLS

Anti-phishing tools are programs created to protect users from phishing attacks. These tools work by analysing the content and structure of the emails and webpages to identify scams. These tools check url status in their phishing database, if the url exists already than it is blocked by the tools [10][13]. The tools used for this research are as follows:-

A. Bitdefender Traffic Light

Bitdefender Traffic Light is a free web browser extension developed by Bitdefender, a cyber-security company founded in 2001. Bitdefender is known for its antivirus and internet security software solutions for home and business users, and its products have won numerous awards for their effectiveness and innovation.

The Traffic Light extension was first released in 2012 and has since been updated to include additional security and privacy features. It is designed to protect users from various online threats, including phishing scams, malware, and malicious websites[14].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Bitdefender Traffic Light uses a combination of content-based and structure-based methods to analyse webpages and determine if they are safe or not. Content-based analysis involves analysing the actual content of a webpage, including text, images, and multimedia, to identify potential threats such as malicious links, phishing scams, or malware. Structure-based analysis, on the other hand, involves examining the underlying code and structure of a webpage to detect suspicious behaviour, such as hidden links or scripts, suspicious redirects, or obfuscated code. Therefore, Bitdefender Traffic Light employs a multi-layered approach that combines both content-based and structure-based analysis to provide robust protection against online threats.

Here are some features of Bitdefender Traffic Light:

1) *Real-time malware detection:* While visiting a website Bitdefender quickly analyses its content and identifies potential threats such as malicious links and malwares.
2) *Safe search results:* While searching something in a search engine, Bitdefender quickly analyses the search results and mark websites with red warning icon that contains malicious content.
3) *Anti-tracking:* Bitdefender Protects user's online privacy by preventing websites from collecting location data and user history.
4) *Works with popular browsers:* Bitdefender works on popular browsers like Chrome, Firefox, Microsoft Edge and Safari.
5) *Lightweight and unobtrusive:* Bitdefender Traffic Light uses very small amount of pc memory and quietly runs in background without slowing down user's browsing experience.
6) *Easy to install and use:* To use Bitdefender Traffic Light user only need to install an extension in browser. It has a very simple User interface.

B. Netcraft

Netcraft is an Internet services company based in Bath, England. Paul Mutton founded it in 1995, and it initially offered web hosting and consulting services to businesses. However, the company is perhaps best known for its internet security and anti-phishing services, which it has been offering since the early 2000s.

Netcraft's anti-phishing services involve monitoring websites for signs of phishing attacks and identifying fake or suspicious websites that may be trying to steal users' personal or financial information[13][14]. The Netcraft extension primarily uses a content-based approach to detect and analyse websites. It examines the content of web pages and analysis the server response headers to identify information about the web server, operating system, and other technical details. It also uses machine learning algorithms to identify potential phishing and fraudulent websites by analysing the structure of URLs, domains, and web content.

Here are some Features of Netcraft:

1) *Blocks phishing sites and other malicious content:* Netcraft checks website that the user wants to visit in the phishing website database and blocks if the site exists in the database.
2) *Displays detailed information about the sites user visit:* Netcraft generates a report of the site user is visiting which includes SSL certificate, hosting provider and domain registration information.
3) *Helps protect against online fraud:* Netcraft uses anomalous traffic patterns technique to detect online fraud and malicious codes.
4) *Blocks malicious JavaScript and other dangerous content:* Netcraft maintains a database of known malicious JavaScript content and uses it to protect users online.
5) *Warns about fake online shopping sites:* Netcraft uses structure based approach which checks the structure of webpage to identify a phishing website.
6) *Identifies the hosting location of a website:* Netcraft uses IP address analysis, DNS analysis and Reverse DNS lookups to identify the host of website and its location.

C. McAfee Web Advisor

McAfee Web Advisor is a browser extension that offers users protection against online threats such as malware, phishing, and other malicious websites[12]. McAfee, a cyber-security company founded in 1987 by John McAfee, develops this extension.

McAfee Web Advisor was launched in 2016 as a free browser extension that provides users with real-time protection against online threats. The extension works with popular web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge.McAfee Web Advisor primarily uses a content-based approach to protect users from potentially harmful websites and online content. This means that it analyses the content of web pages, files, and downloads to determine if they pose a security risk. It uses various techniques such as heuristics, signature detection, and machine learning algorithms to identify potential threats based on their content.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Here are some features of McAfee Web Advisor:

1) *Warns About Risky Websites and Links:* McAfee maintains a database of websites and URLs and uses this database to assign a reputation score to each website. McAfee blocks websites with low reputation score.
2) *Scans Download for Viruses and Other Threats:* McAfee maintains a database of known viruses and other threats. When user downloads a file McAfee checks it against the database to see if it matches any threat.
3) *Offers Secure Search Results:* McAfee assigns safety rating to the search results and checks for malicious links in search results.
4) *Blocks Unwanted and Intrusive Ads:* McAfee Web Advisor contains ad blocker, popup blocker and tracking protection to protect user form unwanted distractions.
5) *Provides Password Protection for Multiple Accounts:* McAfee uses password encryption and two-factor authentication to protect passwords of users.

IV. RESULTS AND ANALYSIS

TABLE I
COMPARISON OF FEATURES OF TOOLS

Feature	Bitdefender Traffic Light	Netcraft	McAfee Web Advisor
Browser Compatibility	Chrome, Firefox and Safari	Chrome, Firefox and Safari	Chrome, Firefox, Edge and Opera
Web Rating System	Yes	Yes	Yes
Blocking	Yes	Yes	Yes
Malware Protection	Yes	Yes	Yes
Tracking Protection	Yes	Yes	No
Ad Blocker	Yes	Yes	No
Password Manager	No	No	No

As table I shows Netcraft lacks some important features such as tracking protection, ad blocker and password manager. Bitdefender traffic light and McAfee web advisor both are feature packed except lack of password manager and Bitdefender's lack of Microsoft edge compatibility. Overall, all websites provide basic security functions like web rating system, blocking phishing websites and malware protection.

After testing the tools separately on 500 websites including 250 legitimate and 250 phishing websites, following results were found:

TABLE II
RESULTS AFTER TESTING THE TOOLS

Tools	TP Rate	FP Rate	TN Rate	FN Rate
Bitdefender Traffic Light	0.996	0.096	0.904	0.004
Netcraft	0.916	0.520	0.480	0.084
McAfee Web Advisor	0.956	0.440	0.560	0.044

TP rate: True Positive rate
FP rate: False Positive rate
TN rate: True Negative rate
FN rate: False Negative rate

Table II shows that Bitdefender traffic light has best true positive, true negative, false positive and false negative rate as compared to McAfee and Netcraft, which makes it the best performing tool.

To find the accuracy of tools following formula was used:-

Accuracy = [(TP rate + TN rate) / (TP rate + FP rate + TN rate +FN rate)]*100

©IJRASET: All Rights are Reserved

TABLE III
ACCURACY OF THE TOOLS

Tool	Accuracy
Bitdefender Traffic Light	95%
Netcraft	69.8%
McAfee Web Advisor	75.8%

As found out Bitdefender traffic light was able to give 95% accuracy in detecting phishing because it has most of the required features and uses a multi-layered approach to detect phishing.
McAfee was able to give 75.80% accuracy because it doesn't check the structure of the webpage which may contain malicious code. Whereas Netcraft performed the worst with 69.80% accuracy because it has limited features and has high false positive rate. Netcraft may not be able to detect latest social engineering attacks

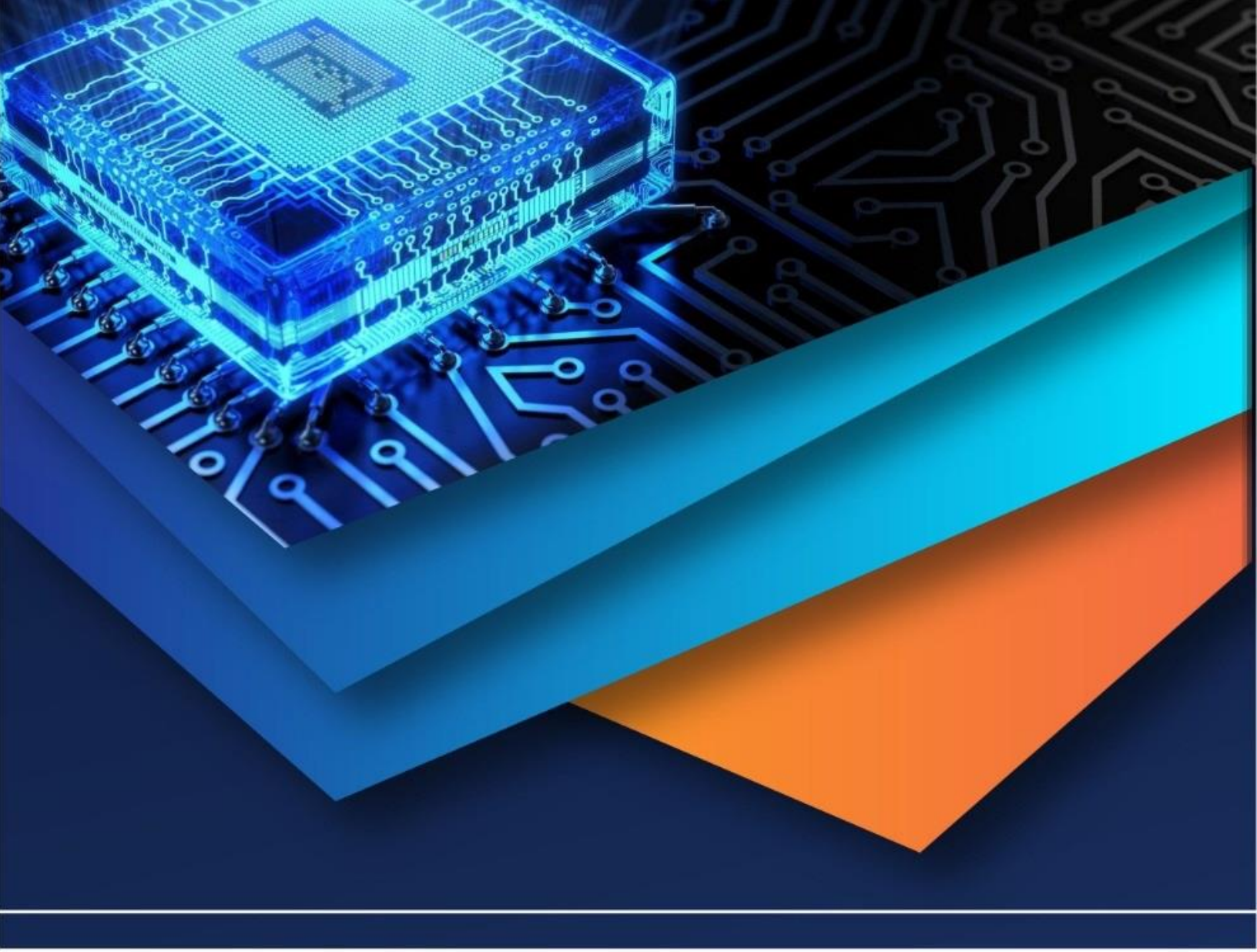
V. CONCLUSIONS AND FUTURE SCOPE

The comparative study of anti-phishing tools has shown that there are a variety of effective solutions available to combat phishing attacks. The evaluation of these tools has been based on several criteria, including ease of use, accuracy, and effectiveness. The results indicate that Bitdefender Traffic Light performs better than others in certain areas, suggesting that selecting the appropriate tool depends on the specific requirements and preferences of the user. The study also emphasizes the importance of raising awareness among users about the risks of phishing attacks and the need to implement appropriate preventive measures.
As technology evolves and new phishing techniques emerge, it is essential to continuously evaluate and update the anti-phishing tools to ensure that they remain effective. Further research can focus on developing more sophisticated tools that use advanced algorithms and artificial intelligence to identify and prevent phishing attacks. Additionally, future studies can examine the effectiveness of anti-phishing tools in different contexts, such as in specific industries or organizations. Moreover, given the increasing reliance on mobile devices, it is crucial to investigate the efficacy of anti-phishing tools for mobile platforms. Ultimately, the future scope of the comparative study of anti-phishing tools is vast, and it has the potential to make a significant contribution to enhancing cyber security and protecting individuals and organizations from the risks of phishing attacks.

REFERENCES

[1] Dr.Radha Damodaram, "Study On Phishing Attacks And Antiphishing Tools," Int. Res. J. Eng. Technol. IRJET, vol. 3, no. 1, pp. 700–705, Jan. 2016.
[2] Grandhi Vanitha, "Detection of Phishing Attack," Int. J. Res. Publ. Rev., vol. 3, no. 11, pp. 569–573, Nov. 2022.
[3] "Anti-Phishing Working Group 2019." [Online]. Available: https://www.apwg.org/trendsreports/
[4] "Phishlabs Phishing Report 2019." [Online]. Available: https://www.phishlabs.com/resources/
[5] Ian Thomas, "IRONSCALES Phishing Survey," The State of Cybersecurity: Phishing on the Rise, Oct. 15, 2021.
[6] Mariadas Ronnie and Jincy Rachel Varghese, "Phishing-Types and Methods for Detection," Int. J. Creat. Res. Thoughts IJCRT, vol. 6, no. 2, pp. 482–486, Apr. 2018.
[7] Bhuvana, Arundhathi S Bhat, Thirtha Shetty, and Mr. Pradeep Naik, "A Study on Various Phishing Techniques and Recent Phishing Attacks," Int. J. Adv. Res. Sci. Commun. Technol. IJARSCT, vol. 11, no. 1, pp. 142–148, Nov. 2021.
[8] "Internet Crime Report," Federal Bureau of Investiation, 2021.
[9] Vaishnavi Bhavsar, Aditya Kadlak, and Shabnam Sharma, "Study on Phishing Attacks," Int. J. Comput. Appl., vol. 182, no. 33, pp. 27–29, Dec. 2018.
[10] T. Venkat Narayana Rao and Sreeja Reddy, "Investigation of Phishing Attacks and Means to Utilize Anti Phishing Techniques," Int. J. Recent Innov. Trends Comput. Commun., vol. 7, no. 2, pp. 5–10, Feb. 2019.
[11] V. Suganya, "A Review on Phishing Attacks and Various Anti Phishing Techniques," Int. J. Comput. Appl., vol. 139, no. 1, pp. 20–23, Apr. 2016.
[12] L. Joy Singh, "A Survey on Phishing and Anti-Phishing Techniques," Int. J. Comput. Sci. Trends Technol. IJCST, vol. 6, no. 2, pp. 62–68, Apr. 2018.
[13] Mayur Bhati and Rashid Khan, "Prevention Approach of Phishing on Different Websites," Int. J. Eng. Technol., vol. 2, no. 7, pp. 1096–1101, Jul. 2012.
[14] Himani Sharma, Er. Meenakshi, and Dr. Sandeep Kaur Bhatia, "A Comparative Analysis And Awareness Survey Of Phishing Detection Tools," IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 2017, pp. 1437–1442.
[15] Gundeep Singh Bindra, "Efficacy of Anti-phishing Measures and Strategies -A research Analysis," Int. J. Comput. Inf. Eng., vol. 4, no. 9, pp. 1409–1415, 2010.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)