IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

Comparative Assessment of Email Phishing Tools

Sagar Bhosale[1] and Arshiya Khan[2]
MCA(Computer Application)[1], Assistant Professor[2],
JSPM University, Pune

Abstract: *Phishing email looks like a normal mail but it is designed to get personal and confidential information of the individual by the hacker. Phishing email is designed to trick the email user to download any software or to visit the link to install virus on their system. As there are various tools available which are used to detect phishing mails still there are some gaps which are not fully covered by these existing tools. This research paper compares and studies the existing email phishing detection tools also analyses the drawbacks of the existing tools, finds accuracy of the tools and compare the overall factors related to the existing tools and gives conclusion.*

Keywords: Phishing Email, Phishing Detection, Cyber Security, Phishing Detection Tools, Privacy

I. INTRODUCTION

Phishing attacks are a major cybersecurity threat, targeting individuals and organizations to steal sensitive information such as passwords, financial data, and personal details. With attackers constantly creating new and sophisticated phishing sites, detecting these threats has become increasingly challenging. The comparative study shows that all tools share some critical gaps. These include difficulty detecting zero-day phishing sites, over-reliance on static blacklists, inconsistent accuracy, limited support for scanning email attachments, privacy concerns due to public uploads, and a lack of real-time automation. These limitations highlight the need for more effective, privacy-oriented, and advance phishing detection solution. Furthermore, most tools only detect but do not remediate threats, leaving organizations to handle takedowns manually. The goal of this research is to study existing email phishing detecting tools, test these tools, find out their accuracy and provide people with the conclusion so that people can use the tools accordingly, it will be helpful for the individuals as well as organizations

Since the mid-1990s, the term “phishing” has been used to identify hackers who use fraudulent emails to “fish for” information from unsuspecting users. However, phishing attacks have become increasingly sophisticated and are now broken down into different types, including email phishing, spear phishing, smishing, vishing, and whaling. Each type is characterized by specific channels and methods of execution email, text, voice, social media, etc. – all with a similar underlying intention.[1]

Phishing Definition: Phishing is the technique of cyberattack where attackers trick users into revealing personal and confidential information such as (passwords, bank details, etc.) to fulfil cyberattacks.

1.1 How email phishing happens:

1. Attacker pick a target. That could be anyone individual, any organization, or a group of people.
2. They create a fake email. The email looks like it is original and from legitimate source.
3. They deliver it to the target. Often many people get the same message; sometimes it’s targeted to one person.
4. Victim is expected to act. The email intended to click a link, open an attachment, or reply with personal information.
5. They steal or infect. If a person click, then it might redirect to the fake site or login page that steals your password, or download malware that let them have access to the device.
6. Attacker use the data for any type of attack. They may steal money, take over accounts, or use your email to phish others..

DOI: 10.48175/IJARSCT-37203

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

Fig 1.1 Process of a phishing attack

1.2 Easy signs an email is a phishing attempt:

1. The sender's email is not regular (extra letters, strange domain).
2. The message is intended to rush or scare you.
3. Links don't match the claimed site when you click them.
4. It asks for sensitive and confidential information through email.
5. The email has bad spelling/grammar or weird formatting.
6. Unexpected attachments

1.3 Precautions to be taken:

1. Don't click links or open attachments from suspicious emails
2. Keep your device updated
3. Use MFA + strong and unique passwords
4. Move your mouse over links in an email to check the real address
5. Verify by contacting the person or company through the official website from other not by using contact information provided in an email

II. LITERATURE REVIEW

Phishing attacks continue to evolve rapidly, using artificial intelligence and social engineering to deceive users and bypass traditional security systems. Recent studies focus on integrating advanced technologies such as machine learning (ML), natural language processing (NLP), and Open-Source Intelligence (OSINT) for better detection and prevention.

An et al. [1] proposed a multilingual phishing email detection model using OSINT and ML, achieving improved accuracy across multiple languages. Liaqat et al. [2] examined phishing in the AI era, emphasizing the role of deep learning models for identifying sophisticated phishing patterns. Choo et al. [3] analyzed VirusTotal's performance, reporting 81.72% phishing detection accuracy, which improved to 97.47% with ML-based aggregation.

LI et al. [6] and Tanti [7] explored detection and prevention strategies, highlighting heuristic and behavioral analysis methods. Olasehinde [8] described the evolution of phishing attacks and their growing complexity, while Putra et al.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

[9] examined recent phishing trends and the rise of targeted attacks. Kavya et al. [10] and Nalawade et al. [11] reviewed hybrid and multi-layered detection frameworks, showing their superiority over single-method systems.

Salloum et al. [12] conducted a large review on NLP-based phishing detection, identifying SVM and deep learning as top-performing models. Khonji et al. [13] and Jadhav and Chandre [14] compared modern phishing detection approaches and stressed challenges such as dataset imbalance, multilingual threats, and real-time adaptability.

Overall, research indicates that no tool achieves complete accuracy. Hybrid systems that combine ML, NLP, OSINT, and real-time threat intelligence offer the most effective protection. This study therefore compares major email phishing tools LinkWall, VirusTotal, ScamX.ai, URLScan.io, Netcraft, Avast, and Kaspersky to assess their accuracy, adaptability, and efficiency.

III. METHODOLOGY

To conduct our research, we began by identifying and reviewing various email phishing detection tools available online. After shortlisting the most relevant and accessible tools, we proceeded to install and test each of them systematically.

For evaluation, we provided multiple types of input data including IP addresses, email samples, QR codes, attachment files, and URLs to assess the detection capabilities of each tool under diverse phishing scenarios. During testing, we carefully recorded the outputs generated by the tools and analysed their performance in terms of accuracy, functionality and usability.

Additionally, we documented the advantages and drawbacks of each tool based on their results and user experience. Finally, by comparing and analysing these findings, we identified the gaps and limitations among the tools, which helped us highlight areas that require further improvement in phishing detection mechanisms and provide the conclusion.

Tools	Dataset	Description	Limitations	Algorithms	Algorithms Description	Accuracy of the Tool
VirusTotal	1.Phishing URLs 2. Attachment file	The phishing email and unauthorized attachment file is provided to the tool and no security vendors flagged this URL and attachment as malicious even after providing malicious URL and attachment.	1. Uploaded files/URLs become public 2. New phishing sites may not be flagged immediately 3. Manual upload/search is time-consuming for bulk emails	1.Multi-engine scanning approach 2. Signature-based detection 3. Heuristic and behavioral analysis	1. Combines results from 70+ antivirus and URL scanners 2. Matches files or links with known malware or phishing signatures. 3. Detects suspicious patterns or unusual code behavior	Current studies evaluate the accuracy of the VirusTotal phishing classification to be at 81.72% [3].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, June 2026 Impact Factor: 8.2

LinkWall	1. EmailID 2. IP address 3. URL 4. QR code	EmailId, IP address, URL and QR code provided to the LinkWall tool and it is giving all the results accurate.	1. It asks for many permissions: location, Google account, phone number etc.	1. Real-time link scanning 2. URL reputation check	1. Analyzes links instantly before users access them 2. Compares links against databases of	Determining the exact or accurate is not possible for LinkWall as
			Intrusive ads inside the app, which degrade experience. Repeated scanning of already known safe links.	Domain age and WHOIS analysis Redirect-chain tracking Heuristic detection	known malicious or phishing websites Flags newly created or suspicious domains often used in phishing Follows multiple redirects to uncover hidden or final malicious destinations Uses rule-based checks to identify unusual or risky link patterns	It depends on various factors.
Scamx.ai	URL Screenshots	Scamx.ai doesn't remove the site itself. When the URL or screenshots are provided it checks the URL with AI + databases, then it checked by the security experts and after confirmation the link is marked as a scam or phishing.	Relies on people reporting scams or phishing incidents. Hidden malicious content inside email attachment may not be identified sometimes.	User-report analysis URL and link scanning Attachment and content review Domain and metadata checks	Accepts phishing or scam reports submitted by users Checks reported URLs against databases of known phishing or scam websites Analyzes email attachments, screenshots or files for suspicious behavior Evaluates domain age, registration details and website metadata for fraud.	Scamx.ai depends on expert reviews and community reports for threat verification and it does not release specific accuracy.
URLScan.io	URL IP Address	When the data is provided to the tool	By default, scans are	Automated browsing	Simulates user interaction by	Specific accuracy is not available publicly

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, June 2026 Impact Factor: 8.2

		it only scans the valid URLs and IPs but not always sometimes even valid URLs are not scanned by the tool	publicly visible on urlscan.ai. Scans are stored permanently which could unintentionally expose organization's investigations or URLs. It's URL-focused you cannot directly upload suspicious attachments to scan. Paid/private scans are available, but the free tier can leak data unintentionally.	Comprehensive data capture Visual and DOM analysis Metadata collection Structural similarity analysis	visiting URLs in a controlled environment Records network activity, including domains, IPs and resources like JavaScript and CSS Takes screenshots and extracts Document Object Model (DOM) content Gathers information such as cookies, JavaScript global variables, and SSL certificate details Detects sites with layouts or code resembling known phishing templates	[15].
Netcraft Phishing Protection	URL IP Address	After entering URL or IP address it detects the malicious sites and blocks them but unable to detect attachments and new links	It doesn't shows the result in the app. Doesn't scan email attachments. Some safe websites may be flagged. Works mostly on links you tap; it doesn't scan all incoming emails automatically.	URL reputation analysis Suspicious content detection Real-time monitoring Anti-phishing toolbar integration	Checks URLs against NetCraft's extensive database of known phishing and malicious websites Looks for phishing indicators in page content, forms, and input fields Continuously scans the web for new phishing sites and updates the database for protection Warns users in browsers when they attempt to visit malicious sites	About 78.4% of threats were reported by Netcraft, which tracks phishing and online scams globally[5].
Avast Antivirus	Email URL	This tool blocks known phishing	New phishing sites or malware	Heuristic analysis	Detects suspicious patterns	Blocked 99% of phishing attempts in a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 10, June 2026 Impact Factor: 8.2

and Security	Phishing file Phishing link	sites, malicious apps, and dangerous links, warns about risky websites, and can prevent malware infections. However, brand-new threats or zero-day phishing links may occasionally slip through and some safe sites can be flagged as suspicious	may sometimes bypass detection. Safe links or apps may occasionally be flagged as risky. Focuses more on apps and links; doesn't deeply scan all email attachments.	Machine learning models Web and email protection	or unusual behavior in files and websites Uses AI-based analysis to identify zero-day malware and phishing threats Scans websites, links, and email attachments in real-time to block phishing attempts.	2022 AV-Comparativ es test [16].
Kaspersky	Email Website URL	Kaspersky scans apps, links, and websites in real time. Blocks known phishing URLs and malicious sites. Monitors device behaviour to detect suspicious activity.	Relies on database ,may miss zero day phishing sites. Sometime shows false negatives or delays in blocking suspicious links.	Behavioral analysis / sandboxing Heuristic analysis Signature-based detection Cloud-based reputation system	Observes program actions in a secure environment to detect malicious activity Identifies suspicious code or behavior patterns even in previously unknown threats Matches files, URLs, and email attachments against a database of known malware and phishing threats Quickly evaluates files and links using Kaspersky Security Network for Reputation and threat assessment	Achieved a 93% detection rate with zero false positives in 2024 and 2025[4].

IV. RESULT

After testing all the selected email phishing detection tools VirusTotal, LinkWall, Scamx.ai, URLScan.io, Netcraft Phishing Protection, Avast Antivirus, and Kaspersky several observations were made based on their accuracy, usability, privacy handling, and detection capability.

4.1. Detection Accuracy and Performance:

1. Avast Antivirus blocks 99% phishing emails of according to the AV-Comparatives report and showed the highest phishing detection accuracy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

2. Kaspersky also provide 93% detection rate showing reliability in real time detection.
3. Netcraft Phishing Protection showed an average of 78.4% phishing threat detection which is good but not at the level of top phishing detection tools.
4. VirusTotal effectively detected phishing URLs and files effectively but failed to detect zero-day threats quickly because of its reliance on signature-based scanning.
5. LinkWall gives accurate results across URLs, IPs and emails but it is dependent on various factors such as database updates, network and permissions this is the reason for not giving exact accuracy measurements.
6. Scamx.ai performed well in identifying phishing links but it lacks automation. It gives results based on human review and community reports, which means delayed verification for new scams.
7. URLScan.io is useful for analyzing and visualizing phishing pages but often skipped valid URLs and lacked attachment-scanning support.

4.2. Usability and Features:

1. Linkwall and VirusTotal provided user-friendly interfaces but required manual uploads which is time consuming and for bulk scanning.
2. Avast and Kaspersky provided easy-to-use apps with real-time protection which makes them more suitable for regular users.
3. Scamx.ai included expert review but was slower to update.
4. URLScan.io offered in-depth technical analysis and also useful for cybersecurity professionals but complex for the regular users.
5. Netcraft integrated directly with browsers but it could not scan attachments and sometimes flagged safe sites.

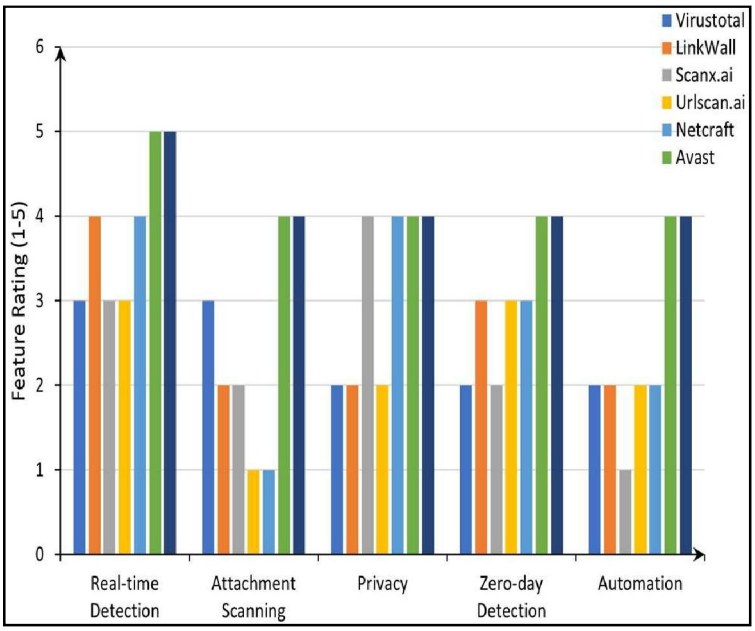

Figure 2 presents a comparative bar graph analysis of six email phishing detection tools — VirusTotal, LinkWall, Scamx.ai, URLScan.io, Netcraft, and Avast — evaluated across five critical feature categories: Real-time Detection, Attachment Scanning, Privacy, Zero-day Detection, and Automation, rated on a scale of 1 to 5.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

In terms of Real-time Detection and Automation, Avast led with the highest rating, supported by its 99% phishing block rate as reported by AV-Comparatives 2022, followed by Kaspersky with a 93% detection rate and zero false positives in 2024–2025. Both tools offer fully automated, continuous background protection without manual intervention. Tools such as VirusTotal, LinkWall, URLScan.io, and Scamx.ai scored low in these categories as they require manual submission for every scan, making them less practical for daily use. VirusTotal reported an accuracy of 81.72%, which improved to 97.47% with ML-based aggregation.

Regarding Attachment Scanning, Avast and Kaspersky again performed best due to their ability to inspect email attachments in real time. Most other tools, particularly URLScan.io, Netcraft, and Scamx.ai, scored poorly as their detection is largely limited to URL-based analysis only.

In the Privacy category, Scamx.ai and Netcraft rated higher as they do not publicly expose user-submitted data. VirusTotal and URLScan.io scored lower despite their reasonable detection accuracies, as both platforms make uploaded files and scan results publicly accessible by default, raising significant privacy concerns.

The Zero-day Detection category recorded the lowest scores across all tools, representing the most critical shared limitation. Even top performers like Avast at 99% and Kaspersky at 93% acknowledged occasional failures against brand-new phishing threats. Netcraft reported 78.4% threat detection, while LinkWall, Scamx.ai, and URLScan.io did not publicly disclose specific accuracy figures, limiting their comparability.

Overall, the graph confirms that no single tool provides complete protection across all feature dimensions. Avast and Kaspersky emerged as the most well-rounded tools in terms of accuracy, automation, and usability, while tools like VirusTotal and URLScan.io serve better as investigative tools for cybersecurity professionals. The consistently poor zero-day detection across all tools highlights the urgent need for more advanced, AI-driven, and privacy-focused phishing detection solutions

4.3 Privacy and Data Handling:

1. Scamx.ai and Netcraft had better privacy management as they do not share users' data publicly.
2. Avast and Kaspersky provided users data privacy while offering strong cloud-based protection.
3. LinkWall needed many permissions such as location and Google account which raised privacy concern.
4. VirusTotal and LinkWall made users uploaded data publicly available which could expose private investigations or internal links.

4.3. Common Limitations Found Across Tools:

1. Many tools could not detect zero-day phishing sites effectively.
2. Many tools relied on databases or blacklists, making them reactive instead of proactive.
3. Some tools lacked attachment scanning and could only detect phishing through URLs.
4. Tools like VirusTotal and URLScan.io made uploaded information publicly visible, raising privacy risks.
5. None of the tools offered automatic remediation they only detected phishing but did not remove or report the malicious source automatically.

IV. DISCUSSION

The results show that while there are many tools available for detecting phishing emails, no single tool provides complete protection. Tools like Avast and Kaspersky lead in terms of accuracy, automation, and ease of use, making them ideal for both individual users and organizations. Avast achieved the highest phishing block rate of 99% according to the AV-Comparatives 2022 report, while Kaspersky followed closely with a 93% detection rate and zero false positives in 2024–2025. Both tools use machine learning, heuristic analysis, and cloud reputation systems, which allow faster detection of new threats.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

On the other hand, tools like VirusTotal, URLScan.io, and LinkWall are more suitable for cyber researchers or IT professionals, as they offer deep analysis and scanning reports but require manual inputs. VirusTotal reported a phishing detection accuracy of 81.72%, which improved significantly to 97.47% when combined with ML-based aggregation, demonstrating its potential as a powerful investigative tool. However, since these tools require manual submission for every scan, they are not practical for daily users who want automatic protection.

Even though tools like Avast at 99% and Kaspersky at 93% are very fast and accurate in finding phishing threats, they don't always show how their systems work, so it's hard for researchers to study them in detail. On the other hand, platforms like VirusTotal and URLScan.io are more open — they share detailed scanning reports that help experts understand and track online threats better. This shows a clear balance between ease of use, openness, and automation — everyday users prefer simple and automatic protection, while cybersecurity professionals look for tools that give them deeper information and control.

Scamx.ai and Netcraft play an important role in community-driven phishing awareness and reporting. Netcraft reported detecting approximately 78.4% of phishing threats globally, reflecting its reasonable but limited capability. Scamx.ai, however, does not publicly disclose a specific accuracy figure as its results depend entirely on human expert review and community-based verification, which limits its ability to detect brand-new phishing sites instantly and makes it difficult to evaluate its performance objectively against other tools.

Privacy was another major concern. Tools that store or share scans publicly, such as VirusTotal with 81.72% accuracy and URLScan.io whose accuracy is not publicly available, can unintentionally expose sensitive information despite their reasonable detection capabilities. LinkWall, whose accuracy cannot be precisely determined due to its dependence on database updates, network conditions, and user-granted permissions, also raised privacy concerns by requiring excessive user permissions such as location access and Google account details. This indicates the need for privacy-centric phishing detection systems that analyze data securely without public sharing

From the findings, it is clear that the current phishing detection ecosystem is fragmented — each tool focuses on certain areas such as URLs, emails, attachments, or domains, but none combines them all in one secure, automated platform. The significant gap in accuracy between the best-performing tools, Avast at 99% and Kaspersky at 93%, and the rest, Netcraft at 78.4% and VirusTotal at 81.72%, along with the complete absence of published accuracy figures for LinkWall, Scamx.ai, and URLScan.io, further highlights the inconsistency across the current ecosystem. These disparities in accuracy, combined with the lack of automation and persistent privacy issues, strongly suggest that future phishing detection tools should combine AI-based prediction, real-time detection, and user data protection to provide comprehensive end-to-end security.

V. CONCLUSION

This research compared different email phishing detection tools and found that while most offer good protection, none are completely reliable. Avast and Kaspersky performed best overall, while tools like VirusTotal, URLScan.io, and Netcraft had specific strengths but limited automation and privacy. The main gaps observed were weak detection of zero-day attacks, poor attachment scanning, and privacy risks. These findings show the need for more automated and privacy-focused phishing detection systems. This study can help users and organizations choose the right tools and guide future work in developing smarter, AI-based solutions. With stronger awareness and better technology, a safer digital environment can be achieved.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

REFERENCES

[1] Panharith An, Rana Shafi, Tionge Mughogho, Onyango Allan Onyango , "Multilingual Email Phishing Attacks Detection using OSINT and Machine Learning", arXiv:2501.08723v1 [cs.CR] 15 Jan 2025, https://arxiv.org/abs/2501.08723

[2] Muhammad Saeed Liaqat, Gohar Mumtaz, Nazish Rasheed and Zeeshan Mubeen, "Exploring Phishing Attacks in the AI Age: A Comprehensive Literature Review", Journal of Computing & Biomedical Informatics, Vol. 07, 2024, https://www.jcbi.org/index.php/Main/article/vi ew/567/534

[3] Choo, E., Nabeel, M., De Silva, R., Yu, T., & Khalil, I. (2022). "A large scale study and classification of VirusTotal reports on phishing and malware URLs". arXiv preprint arXiv:2205.13155. Retrieved from https://arxiv.org/abs/2205.13155

[4] Kaspersky Website : https://www.kaspersky.com/about/pressreleases/kaspersky-premium-takes-gold-in-2024- anti-phishing-test-by-av-comparatives.

[5] Netcraft Website :https://www.netcraft.com/

[6] LI, Daoming, CHEN, Qiang, WANG, Lun, "Phishing Attacks : Detection and Prevention Techniques", Journal of Industrial Engineering and Applied Science, Vol. 02, 2024, https://www.suaspress.org/ojs/index.php/JIEA S/article/view/v2n4a08/v2n4a

[7] Rajesh Tanti, "Phishing Attack: A Case Study and their Prevention Techniques", International Journal for Multidisciplinary Research (IJFMR), Vol. 06, October 2024, https://www.ijfmr.com/papers/2024/5/29087.p df

[8] Tolamise Olasehinde, "The Evolution of Phishing Attacks : Tactics and Countermeasures", October 2024, https://www.researchgate.net/publication/3850 91892_THE_EVOLUTION_OF_PHISHING_ ATTACKS_TACTICS_AND_COUNTERME ASURES

[9] Fuzan Prasetyo Eka Putra1, Ubaidi, Achmad Zulfikri, Goffal Arifin, Revi Mario Ilhamsyah, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study", Brilliance Research of Artificial Intelligence , Vol. 04, May 2024 , https://www.researchgate.net/publication/3831 93964_Analysis_of_Phishing_Attack_Trends_ Impacts_and_Prevention_Methods_Literature_ Study

[10] S. Kavya, D. Sumathi, "Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection", December 2024, https://www.researchgate.net/publication/3872 73858_Staying_ahead_of_phishers_a_review_of_recent_advances_and_emerging_methodol ogies_in_phishing_detection

[11] Prof. V. S. Nalawade, Ms. Bankar Nandini Sanjay, Ms. Mohite Pooja Nanasaheb, Mr. Saykar Vaibhav Vikram, Mr. Padhar Tejas Khandeshwar, "Survey on Phishing Attack Prevention Techniques Across Multiple Applications: Current Strategies, Challenges, and Future Trends", International Journal of Electrical, Electronics and Computer Systems, Vol. 13, 2024, https://journals.mriindia.com/index.php/ijeec s/article/download/10/5

[12] Said Salloum, Tarek Gaber, Sunil Vadera, Khaled Shaalan, "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques", IEEE, Vol. 10, June 2022, https://www.researchgate.net/publication/3613 00183_A_Systematic_Literature_Review_on_ Phishing_Email_Detection_Using_Natural_La nguage_Processing_Techniques

[13] Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones, "Phishing Detection : A Literature Survey", ResearchGate, April 2013, https://www.researchgate.net/publication/2568 41808_Phishing_Detection_A_Literature_Survey

[14] Ashvini Jadhav, Pankaj R. Chandre, "Survey and comparative analysis of phishing detection techniques: current trends, challenges, and future directions", IAES International Journal of Artificial Intelligence (IJAI), Vol. 14, April 2025, https://ijai.iaescore.com/index.php/IJAI/article /view/25990/14414

[15] URLScan.io Website : https://urlscan.io

[16] Avast Website : https://blog.avast.com/avast-anti-phishingproducts-outperform-others-avast

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

[17] Sanjog S. Harihar, Dr. Mahesh Potdar, "A Comprehensive Analysis of Phishing Challenges and Ai Solutions Adopted by it Organizations", Journal of Neonatal Surgery, Vol. 14, Issue 22s (2025), https://www.jneonatalsurg.com/index.php/jns/a rticle/view/5427

[18] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, Jari Porras, "Mitigation strategies against the phishing attacks: A systematic literature review", https://www.sciencedirect.com/science/article/pii/S0167404823002973

[19] Asad Abbas, "Evolving Phishing Defense : Innovative Defense Mechanisms and Effective Measurement Strategies", (PDF) Evolving Phishing Defense: Innovative Defense Mechanisms and Effective Measurement Strategies

[20] Jafer Hera, "Phishing Defense Mechanisms: Strategies for Effective Measurement and Cyber Threat Mitigation", September 2024, ResearchGate, (PDF) Phishing Defense Mechanisms: Strategies for Effective Measurement and Cyber Threat Mitigation

[21] James Carter, Olivia Smith, "The Growing Threat of Phishing Attacks and How to Prevent Them", International Journal of Emerging Trends in Information Technology (IJEIT), Vol. 1, Issue 1, April 2025

[22] Tanusree Sharma , "Evolving Phishing Email Prevention Techniques: A Survey to Pin DownEffective Phishing Study Design Concepts", Published 2021, https://www.academia.edu/66864809/Evolving Phishing_Email_Prevention_Techniques_A_ Survey_to_Pin_Down_Effective_Phishing_Stu dy_Design_Concepts

[23] Ashvini Jadhav, Pankaj R. Chandre, "Survey and comparative analysis of phishing detection techniques: current trends, challenges, and future directions", IAES International Journal of Artificial Intelligence (IJ-AI) p 853 Vol. 14, No. 2, April 2025, https://ijai.iaescore.com/index.php/IJAI/article /view/25990/14414

[24] Jikesh Thapa, Gurrehmat Chahal, S , erban Voinea Gabreanu, Yazan Otoum, "Phishing Detection in the GenAI Era: Quantized LLMs vs Classical Models", https://arxiv.org/pdf/2507.07406

[25] Adrian-Viorel ANDRIU, "Adaptive Phishing Detection: Harnessing the Power of Artificial Intelligence for Enhanced Email Security", Romanian Cyber Security Journal, Vol. 5, Spring 2023, https://rocys.ici.ro/documents/89/2023_spring _article_1.pdf

[26] Nina Marshall, Daniel Sturman * , Jaime C. Auton, "Exploring the evidence for email phishing training: A scoping review", Computers & Security, Vol.139, April 2024, https://www.sciencedirect.com/science/article/pii/S01674048230060