Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

THE EVOLUTION OF RESEARCH ON PHISHING: A BIBLIOMETRIC ANALYSIS (2005–2025)

Norlizawati Ghazali[1*], Ina Suryani Ab Rahim[2], Syed Zulkarnain Syed Idrus[3]

[1,2,3] Department of Languages and General Studies, Universiti Malaysia Perlis, Malaysia
Email: norlizawati@uitm.edu.my inasuryani@unimap.edu.my syzul@unimap.edu.my
[2] Academy of Language Studies, Universiti Teknologi MARA Cawangan Perlis, Malaysia
Email: norlizawati@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 30.06.2025
Revised date: 21.07.2025
Accepted date: 11.08.2025
Published date: 01.09.2025

To cite this document:

Ghazali, N., Ab Rahim, I. S., & Syed Idrus, S. Z. (2025). The Evolution Of Research On Phishing: A Bibliometric Analysis (2005–2025). *Journal of Information System and Technology Management, 10* (40), 19-33.

DOI: 10.35631/JISTM.1040002

Abstract:

Phishing has emerged as one of the most pervasive cyber threats in the digital age, evolving in both technical sophistication and psychological manipulation. While considerable research has been conducted on phishing detection and user susceptibility, a comprehensive bibliometric analysis of this field remains limited. This study addresses that gap by examining the evolution of phishing-related research from 2005 to 2025 through a systematic bibliometric approach. Using data extracted from the Scopus database (n = 1196) and analyzed through *Scopus Analyzer*, *OpenRefine*, and *VOSviewer*, the study explores annual publication trends, identifies the most cited articles, highlights prolific authors and contributing countries, and maps keyword co-occurrence, co-authorship, and co-citation networks. There has been a significant surge in publication output post-2016, with peak contributions between 2020 and 2024, likely influenced by global digitalization and the COVID-19 pandemic. The most cited works emphasize machine learning, persuasion tactics, and phishing susceptibility. India, the United Kingdom and the United States emerged as leading contributors, with the United States exhibiting the highest total link strength in collaborative networks. Among the 2000+ keywords identified, "phishing," "machine learning," "cybersecurity," "phishing detection," and "social engineering" were most prominent. Keyword co-occurrence mapping illustrates a dual focus on technical detection and human-centered analysis. The co-authorship analysis shows moderate international collaboration, concentrated among select academic hubs, while co-citation analysis reveals key intellectual influencers shaping the field. The findings present an in-depth overview of the intellectual structure and worldwide development of phishing research, highlighting the interdisciplinary nature of the field and informing future research directions for cybersecurity scholars and practitioners.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

Keywords:

Phishing, Bibliometric Analysis, Cybersecurity, Machine Learning, Research Trends

Introduction

Over the last two decades, phishing has become one of the most pervasive and destructive forms of cyberattacks. Hence, this study aims to offer a thorough analysis of phishing trends from 2000 to 2025, highlighting the evolution of phishing techniques, the impact on various sectors, and the effectiveness of countermeasures. The value of this research stems from its potential to inform cybersecurity strategies and enhance the resilience of individuals and organizations against phishing threats.

Phishing attacks exploit human vulnerabilities by masquerading as legitimate communications to steal sensitive information or deploy malicious software. The frequency and sophistication of these attacks have increased dramatically, with notable surges during periods of social disturbance, for instance, the COVID-19 pandemic (Hoheisel et al., 2023) (Carrasco-Farré, n.d.). Phishing attacks reached a record high in the third quarter of 2022, as reported by the Anti-Phishing Working Group (APWG), underscoring the growing threat. Despite advancements in email filtering technologies by major email clients like Gmail, Yahoo, and Outlook, phishing continues to evade detection due to its evolving nature (Chien & Khethavath, 2023). This persistent threat necessitates ongoing research to understand phishing trends and develop more effective countermeasures.

Recent studies have provided valuable insights into the characteristics and trends of phishing emails. For instance, an analysis of phishing emails targeting universities revealed a shift from security-focused phishing to scams reflecting routine university life, for instance, job offer scams (Morrow, 2024). This study also identified common persuasive appeals, such as authority and scarcity, and noted a decrease in spelling errors over time, indicating increased sophistication in phishing tactics (Morrow, 2024). Another study highlighted the impact of the COVID-19 pandemic on phishing trends, with a significant increase in phishing emails exploiting pandemic-related themes (Hoheisel et al., 2023). These findings emphasize the adaptability of phishing schemes to current events and the importance of context-aware detection mechanisms.

Machine learning techniques have been utilized to improve phishing detection, yielding varying levels of success. Experiments focusing on feature extraction and classification have shown promise, but real-world datasets often present challenges that prefetched datasets do not (Chien & Khethavath, 2023). Additionally, the effectiveness of machine learning models can diminish over time as phishing tactics evolve, necessitating continuous updates and improvements (Barreiro Herrera & Camargo Mendoza, 2022). Thus the integration of brand information and the use of diverse detection methods have been suggested to improve the durability and effectiveness of phishing detection models.

The landscape of phishing attacks has seen significant changes in recent years. A study analyzing phishing sites targeting Japanese users identified major attack groups and their strategies, offering vital insights for prioritizing countermeasures (Alkhalil et al., 2021). BP1,

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

the most active group, chiefly targeted banking institutions, while another group directed their efforts at credit card companies, indicating varied attack patterns (Alkhalil et al., 2021). This source-based classification approach highlights the importance of understanding the specific tactics used by different phishing groups to develop targeted defences.

The rise of remote working due to the COVID-19 pandemic has further exacerbated the phishing threat, with employees becoming prime targets for phishing emails. The increased reliance on digital communication has created new vulnerabilities, making it imperative for organizations to enhance their cybersecurity awareness and training programs (Akdemir & Yenal, 2021). Studies have shown that individuals often struggle to detect modern phishing emails, emphasizing the necessity for enhanced training and awareness initiatives (Akdemir & Yenal, 2021).

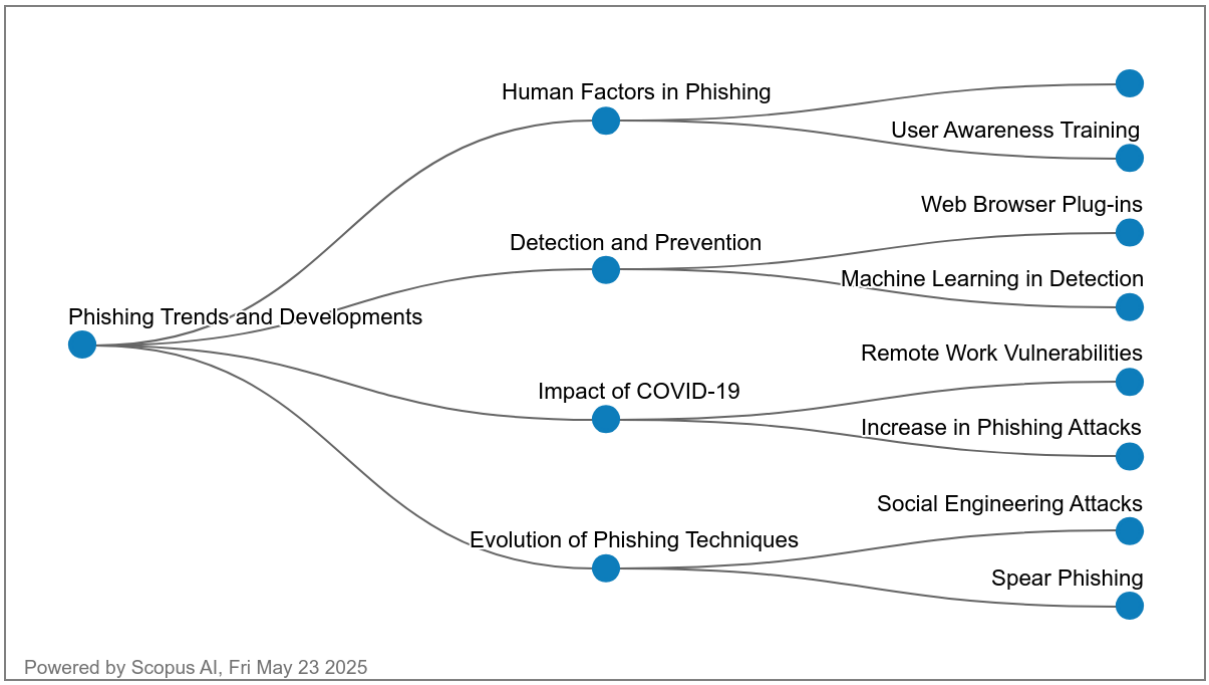

Figure 1: Phishing Trends And Analysis by Scopus AI

Research Question

1. What are the research trends in phishing studies according to the year of publication?
2. What are the most cited articles?
3. What are the top 10 publications by country?
4. What are the popular keywords related to the study?
5. What is the co-authorship network by country?

Methodology

Bibliometrics involves gathering, organizing, and analyzing bibliographic data from scientific publications (Alves et al., 2021; Assyakur & Rosa, 2022; Verbeek et al., 2002). Beyond basic statistics, such as identifying publishing journals, publication years, and leading authors (Wu & Wu, 2017), bibliometrics comprises more detailed techniques, such as document co-citation analysis. Executing a rigorous literature review necessitates a systematic and iterative methodology involving the strategic selection of appropriate keywords, comprehensive literature retrieval, and meticulous analytical procedures. This structured approach facilitates

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

the development of an exhaustive bibliographic compilation and ensures the generation of robust and credible findings (Fahimnia et al., 2015). With this in mind, the research emphasized high-impact publications, as they provide meaningful insights into the theoretical frameworks that shape the research field. To ensure data accuracy, Scopus served as the primary source for data collection (Al-Khoury et al., 2022; di Stefano et al., 2010; Khiste & Paithankar, 2017). Additionally, to retain quality, the research only considered articles published in peer-reviewed academic journals, deliberately excluding books and lecture notes. Bibliometrics entails the collection, organization, and analysis of bibliographic data from scientific literature (Alves et al., 2021; Assyakur & Rosa, 2022; Verbeek et al., 2002). In addition to basic statistical measures such as identifying publication years, prominent authors, and source journals (Wu & Wu, 2017), bibliometric analysis incorporates advanced methods like document co-citation analysis. A rigorous and iterative process is essential for conducting a robust literature review, involving the careful selection of relevant keywords, comprehensive literature searches, and detailed analysis. This methodology facilitates the development of an extensive bibliography and ensures reliable outcomes (Fahimnia et al., 2015). Guided by this framework, the present study emphasized high-impact publications, as they offer valuable insights into the theoretical foundations of the research domain. To guarantee data accuracy, Scopus was employed as the primary data source (Al-Khoury et al., 2022; di Stefano et al., 2010; Khiste & Paithankar, 2017). Furthermore, to uphold the quality of the analysis, only peer-reviewed journal articles were included, with books and lecture notes intentionally excluded (Gu et al., 2019). Using Elsevier's Scopus, known for its broad coverage, publications were collected from 2020 through December 2023 for further analysis.

Data Search Strategy

This study employed a screening sequence to determine the search terms for article retrieval. The study was initiated by querying the Scopus database TITLE (phishing) AND (LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ARTS") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "PSYC")), thereby assembling 1196 articles.

Table 2: The Search String

Scopus	TITLE (phishing) AND PUBYEAR > 2004 AND PUBYEAR < 2026 AND (LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "ARTS"))

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

Table 2: The Selection Criterion For Searching

Criterion	Inclusion	Exclusion
Time line	2004 – 2025	< 2004
Subject	Decision Sciences Social Sciences Business, Management and Accounting Psychology Economics, Econometrics and Finance Arts and Humanities	

Data Analysis

VOSviewer serves as a user-friendly bibliometric software established by Nees Jan van Eck and Ludo Waltman at Leiden University, Netherlands (van Eck & Waltman, 2010a, 2017). It is widely used for the visualization and analysis of scientific literature, with a focus on generating intuitive network visualizations, clustering related items, and producing density maps. The tool's flexibility supports the exploration of co-authorship, co-citation, and keyword co-occurrence networks, offering researchers a comprehensive view of research landscapes. Its interactive interface and regular updates facilitate efficient and dynamic navigation of large datasets. With features such as metric computation, customizable visualizations, and compatibility with various bibliometric data sources, VOSviewer serves as a valuable tool for scholars aiming to gain observations into complex research fields.

A key strength of VOSviewer lies in its ability to convert complex bibliometric datasets into visually accessible maps and charts. With a primary focus on network visualization, the software demonstrates high efficacy in clustering thematically related elements, examining keyword co-occurrence structures, and generating density-based visual representations. Its user-friendly interface facilitates efficient navigation and exploration of scholarly landscapes for both novice and experienced researchers. The ongoing enhancement of VOSviewer ensures its continued relevance and prominence in bibliometric research, offering advanced analytical capabilities through metric computations and customizable visual outputs. Its flexibility in accommodating various forms of bibliometric data, including co-authorship and citation networks, underscores its utility as a robust and indispensable instrument for scholars aiming to derive comprehensive and nuanced insights within their respective research fields.

Datasets containing information such as title, publication year, journal, author name, citations, as well as keywords in PlainText format were retrieved from the Scopus database, covering the year 2004 to December 2024. Consequently, these datasets were subsequently assessed utilizing VOSviewer software (version 1.6.19). Utilizing VOS clustering as well as mapping techniques, the software enabled the generation and examination concerning bibliometric maps. To substitute for the Multidimensional Scaling (MDS) approach, VOSviewer places items in low-dimensional spaces, which ensures that the distance between any two items represents their degree of similarity as well as relatedness (van Eck & Waltman, 2010b). In this regard, VOSviewer shares conceptual similarities with MDS (Appio et al., 2014). However, unlike MDS—which typically relies on similarity measures, for example, Jaccard indices and cosine—VOS implements a more suitable method for normalizing co-occurrence frequencies,

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

namely Association Strength (AS_{ij}), which is measured as described by van Eck & Waltman (2007):

$$AS_{ij} = \frac{C_{ij}}{w_i w_j},$$

where it is "proportional to the ratio between on the one hand the observed number of co-occurrences of i and j and on the other hand the expected number of co-occurrences of i and j under the assumption that co-occurrences of i and j are statistically independent" (van Eck & Waltman, 2007).

Findings

RQ1: What Are The Research Trends In Phishing Studies According To The Year Of Publication?

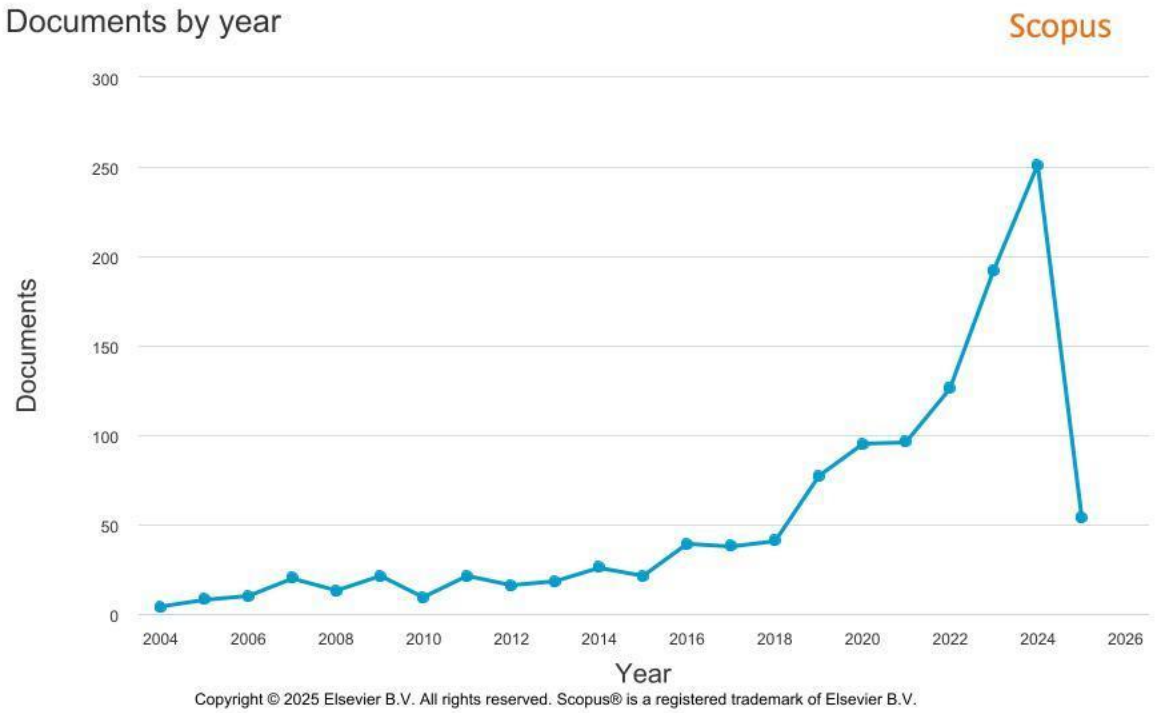

Figure 2: Trends Of Research In Phishing By Years

The longitudinal analysis of phishing-related publications from 2004 to 2025 reveals a marked upward trajectory in scholarly interest, reflecting the growing concern over cyber deception in an increasingly digital world. Initial research activity in the early 2000s was sparse, with fewer than 10 publications annually until 2006. A modest increase is observable between 2007 and 2015, with an average of 15 to 20 publications per year, suggesting a gradual recognition of phishing as a research-worthy phenomenon. However, the period from 2016 onward marks a notable surge, particularly between 2020 and 2024, where annual publications rose sharply, from 77 in 2019 to a peak of 251 in 2024. This exponential growth aligns with global shifts, such as heightened digital engagement during the COVID-19 pandemic, increased phishing incidents, and the diversification of research approaches to incorporate behavioral, linguistic,

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

and educational dimensions. Notably, the proportion of total publications in 2023 and 2024 alone accounts for over one-third of the entire dataset, indicating a significant surge in scholarly momentum. The slight dip observed in 2025 may be attributable to the partial indexing of that year's data at the time of analysis, rather than an actual decline in academic output. Collectively, these findings indicate that phishing, particularly through email, has transitioned from a niche topic within cybersecurity to a multifaceted area of inquiry intersecting with the social sciences, linguistics, and digital literacy.

Table 3: Total Occurrences And Percentage By Year

Year	Total	Percentage	Year	Total	Percentage
2004	4	0.33	2015	21	1.76
2005	8	0.67	2016	39	3.26
2006	10	0.84	2017	38	3.18
2007	20	1.67	2018	41	3.43
2008	13	1.09	2019	77	6.44
2009	21	1.76	2020	95	7.94
2010	9	0.75	2021	96	8.03
2011	21	1.76	2022	126	10.54
2012	16	1.34	2023	192	16.05
2013	18	1.51	2024	251	20.99
2014	26	2.17	2025	54	4.52

RQ2: What Are The Most Cited Articles?

The analysis of the most cited articles in phishing research reveals a diverse and interdisciplinary landscape, encompassing economics, psychology, information systems, cybersecurity, and user behavior. Leading the list is *Phishing for Phools: The Economics of Manipulation and Deception* by Akerlof and Shiller (2015), cited 451 times, which offers a macroeconomic lens on deceptive practices, highlighting how systemic vulnerabilities enable manipulation across markets, including digital contexts. Vishwanath et al.'s (2011) article in *Decision Support Systems*, with 317 citations, proposes an integrated information processing model that explains individual differences in phishing susceptibility, effectively linking cognitive theory and cybersecurity. Notably, Chiew et al.'s (2019) machine learning-based detection framework published in *Information Sciences* garnered 291 citations, demonstrating the continuing significance of hybrid technical approaches. Complementing these, Arachchilage and Love (2014) emphasized user awareness in their study published in *Computers in Human Behavior*, while Aleroud and Zhou's (2017) comprehensive survey in *Computers and Security* synthesized countermeasure techniques. Collectively, these high-impact studies underscore the dual trajectory of phishing research: one that integrates behavioral and psychological theories to understand victimization, and another that leverages computational advances for phishing detection. This citation pattern also illustrates the growing acknowledgment of socio-technical perspectives in addressing cyber deception.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

Table 4: The Most Cited Authors

Authors	Title	Year	Source title	Cited by
Akerlof G.A.; Shiller R.J. (Akerlof & Shiller, 2015)	Phishing for phools: The economics of manipulation and deception	2015	Phishing for Phools: The Economics of Manipulation and Deception	451
Vishwanath A.; Herath T.; Chen R.; Wang J.; Rao H.R. (Vishwanath et al., 2011)	Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model	2011	Decision Support Systems	317
Chiew K.L.; Tan C.L.; Wong K.; Yong K.S.C.; Tiong W.K. (Chiew et al., 2019)	A new hybrid ensemble feature selection framework for a machine learning-based phishing detection system	2019	Information Sciences	291
Arachchilage N.A.G.; Love S. (Arachchilage & Love, 2014)	Security awareness of computer users: A phishing threat avoidance perspective	2014	Computers in Human Behavior	234
Aleroud A.; Zhou L. (Aleroud & Zhou, 2017)	Phishing environments, techniques, and countermeasures: A survey	2017	Computers and Security	214
Dodge Jr. R.C.; Carver C.; Ferguson A.J. (Dodge Jr. et al., 2007)	Phishing for user security awareness	2007	Computers and Security	210
Caputo D.D.; Pfleeger S.L.; Freeman J.D.; Johnson M.E. (Caputo et al., 2014)	Going spear phishing: Exploring embedded training and awareness	2014	IEEE Security and Privacy	206
Wright R.T.; Marett K. (Wright & Marett, 2010)	The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived	2010	Journal of Management Information Systems	203

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

Alsharnouby M.; Alaca F.; Chiasson S. (Alsharnouby et al., 2015)	Why phishing still works: User strategies for combating phishing attacks	2015	International Journal of Human Computer Studies	198
Wang J.; Herath T.; Chen R.; Vishwanath A.; Rao H.R. (Alkhalil et al., 2021c)	Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email	2012	IEEE Transactions on Professional Communication	177

RQ3: What Are The Top 10 Publications By Country?

The distribution of phishing-related publications by country reveals a significant global engagement with the topic, with a notable concentration in technologically advancing and digitally connected regions. India leads with 305 publications, reflecting the country's rapid digital transformation and corresponding concerns over cybersecurity vulnerabilities, especially in the financial and governmental sectors. The United States follows closely with 287 documents, underscoring its longstanding leadership in cybersecurity research and its multifaceted approach to phishing, from technical defences to behavioral studies. The United Kingdom, China, and Australia contribute 84, 77, and 51 publications, respectively, indicating strong academic interest in phishing threats, likely driven by public policy concerns and widespread digital service use. Malaysia (40), Germany (30), Saudi Arabia (29), and Indonesia (28) also demonstrate growing scholarly involvement, suggesting that phishing is increasingly perceived as a critical national concern across both developed and developing nations. This global distribution highlights the transnational nature of phishing threats and underscores the importance of international collaboration in developing holistic countermeasures that consider not only technological dimensions but also linguistic, educational, and sociocultural contexts.

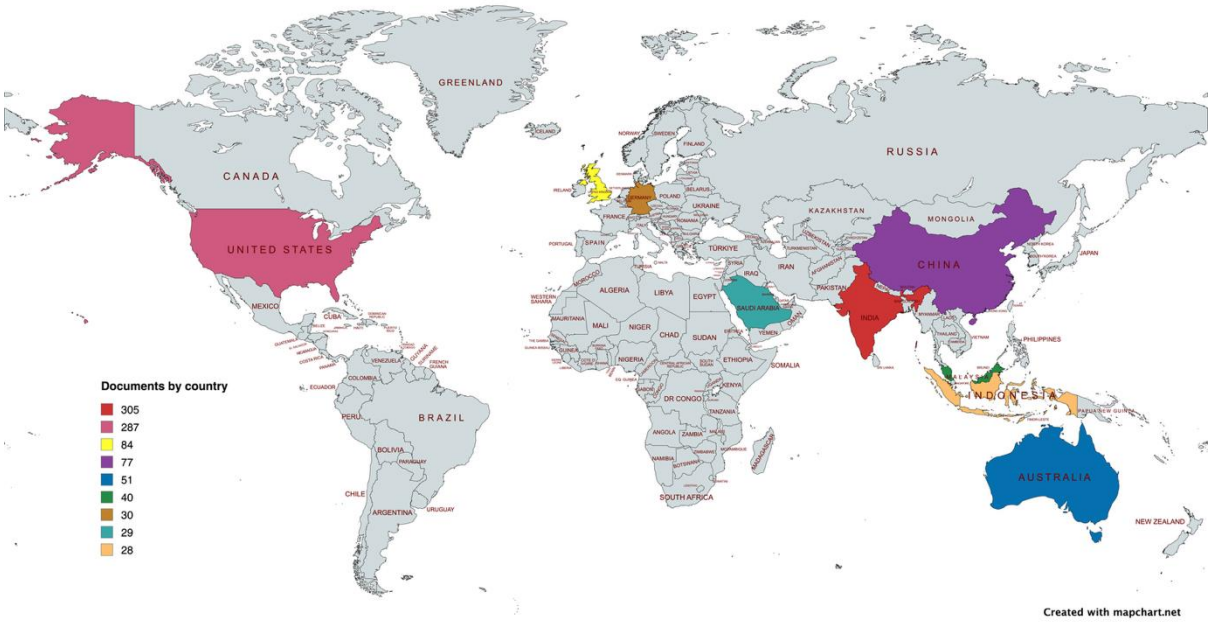

Figure 3: The Distribution Of Phishing-Related Publications By Country

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

RQ4: What Are The Popular Keywords Related To The Study?

Table 5: The Popular Keyword Occurrences And Total Link Strength

No	Keyword	Occurrences	Total Link Strength
1	Phishing	464	801
2	Machine Learning	226	576
3	Cybersecurity	132	281
4	Phishing Detection	129	252
5	Deep Learning	79	216
6	Social Engineering	79	178
7	Phishing Attacks	59	106
8	Classification	43	127
9	Random Forest	43	134
10	Feature Selection	29	70

The keyword co-occurrence network generated through VOSviewer reveals a robust and interdisciplinary thematic landscape in phishing research from 2005 to 2025. Central to the network is the term "phishing" with the highest frequency (464 occurrences) and the strongest total link strength (801), underscoring its foundational role in shaping the research domain. Closely associated nodes include "cybersecurity" (132 occurrences, 281 strength), "machine learning" (226, 576), "phishing detection" (129, 252), and "deep learning" (79, 216), highlighting a dominant technical cluster focused on automated detection methods and algorithmic interventions. Within this cluster, terms like "feature selection," "random forest," and "support vector machine" indicate intensive exploration of classification and optimization techniques.

Another notable subnetwork revolves around human-centric and psychological themes, featuring terms such as "phishing susceptibility" (24, 34), "natural language processing" (24, 55), "social engineering" (79, 178), "persuasion," "trust," and "personality traits." These co-occurrences point to a growing scholarly interest in the cognitive and communicative mechanisms that phishing attacks exploit. The emergence of keywords such as "anti-phishing training," "usable security," and "security awareness" further supports the field's shift toward behavioral interventions and educational countermeasures.

Additionally, newer trends are observable in the inclusion of keywords such as "blockchain," "xgboost," "bert," and "convolutional neural networks," reflecting the integration of state-of-the-art technologies into phishing detection research. The presence of "email phishing," "spear phishing," and "mobile phishing" illustrates a diversification of phishing modalities, while keywords like "victimization," "fraud," and "identity theft" ground the network in socio-legal and psychological consequences.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

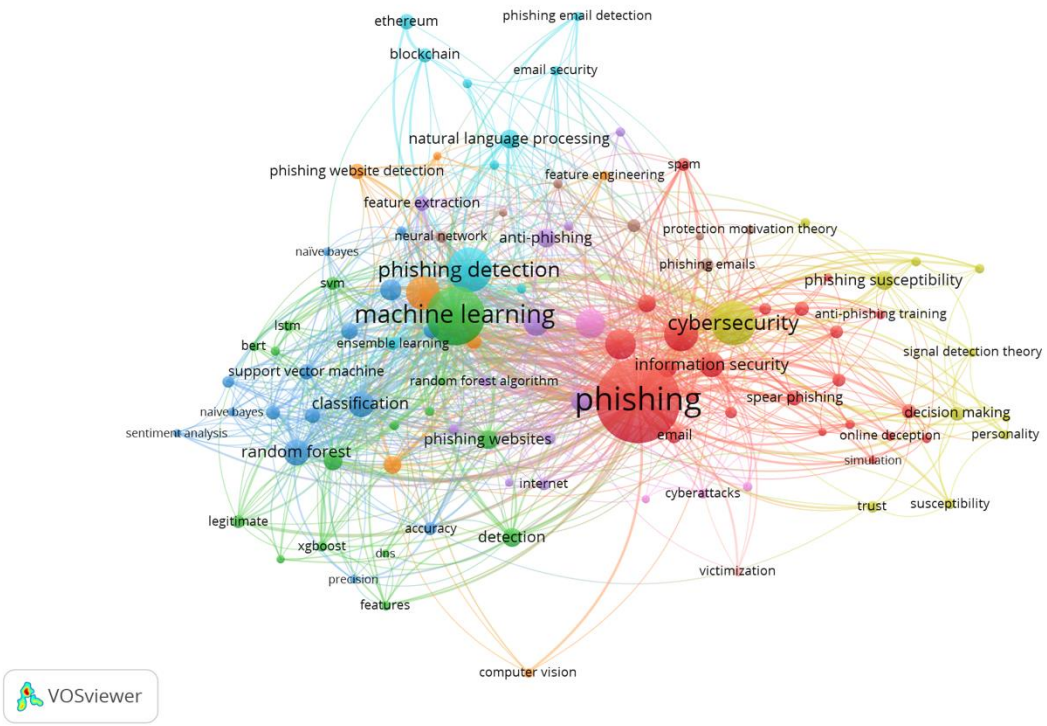

Figure 4: The Popular Keywords Related To The Study

Overall, the co-occurrence map delineates distinct thematic clusters—technical, behavioral, educational, and social—and reflects increasing interdisciplinarity and methodological sophistication in phishing research. The high link strengths and dense interconnections suggest a mature and evolving knowledge network that bridges computer science, linguistics, psychology, and cybersecurity policy.

RQ5: What Is The Co-Authorship Network By Country?

The co-authorship data emphasizes the emergence of a globally interconnected research network, with certain countries acting as key nodes of innovation, while others show strong local engagement but limited cross-border interaction. The data underscores the importance of fostering international partnerships to enhance the breadth and depth of phishing-related research, particularly in underrepresented regions.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

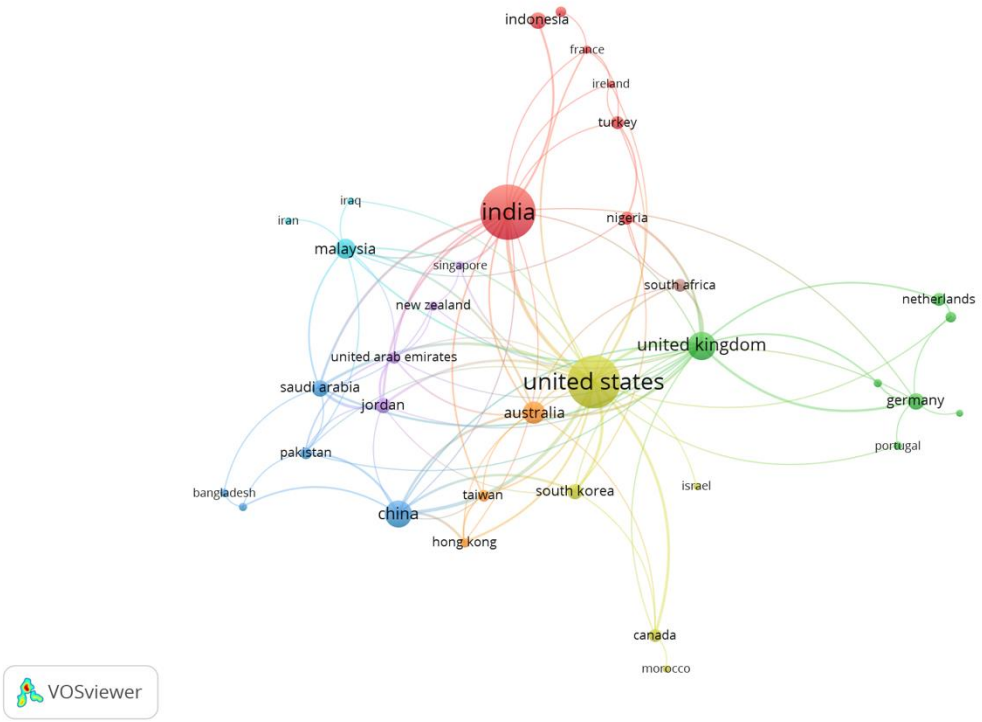

Figure 5: The Co-Authorships Network By Country

The co-authorship network by country, as revealed through VOSviewer, reflects a complex and globally distributed research landscape in phishing studies between 2005 and 2025. The United States leads with 286 documents and the highest citation count (6540), as well as the greatest total link strength (64), highlighting its pivotal role in influencing global research discourse and promoting broad international collaborations. India, with the highest document output (306) and 2536 citations, also demonstrates strong engagement in phishing research, although its total link strength (37) suggests comparatively less collaboration intensity than the United States or the United Kingdom.

The United Kingdom ranks third in terms of influence, contributing 83 publications and achieving 2300 citations with a high total link strength (39), signifying its critical position in collaborative networks. Other notable contributors include China (76 documents, 895 citations, link strength 30), Saudi Arabia (29 documents, 599 citations, link strength 23), and Jordan (26 documents, 590 citations, link strength 22), each playing active roles in regional and transnational research partnerships. Australia, Malaysia, Germany, and South Korea also exhibit notable output and moderate to strong co-authorship links, reflecting their growing roles in the cybersecurity research ecosystem.

Meanwhile, countries like Canada (905 citations on 17 documents) and the Netherlands (681 citations on 18 documents) show high citation impact relative to their document output, indicating the influence and quality of their contributions despite smaller volumes. In contrast, some nations such as Bangladesh, Brazil, and the Philippines demonstrate limited collaboration (total link strength ≤ 2), suggesting the need for enhanced integration into global research frameworks.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

Conclusion

This study aimed to examine the evolution of phishing research over a two-decade span, with the primary objective of identifying publication trends, prominent contributors, thematic focus areas, and collaborative networks. Through bibliometric analysis of 1,196 documents retrieved from the Scopus database, several key patterns and insights emerged. The findings revealed a steady increase in publication activity, with a marked surge beginning in 2016 and peaking in the years 2020–2024, indicating heightened global attention toward phishing in response to increased digital vulnerability. Among the most influential works, studies emphasizing behavioral models, economic manipulation, and machine learning detection frameworks stood out as foundational texts. The United States, India, and the United Kingdom were the top-performing countries, distinguished by both research productivity and robust global research networks, as indicated by co-authorship links.

The keyword co-occurrence analysis demonstrated the dominance of terms, for instance, "phishing," "machine learning," and "cybersecurity," pointing to a dual focus on technical innovation and human susceptibility. Thematic clusters revealed in the analysis suggest that phishing research is both technologically driven and psychologically grounded. By synthesizing this landscape, the study contributes a macro-level understanding of phishing scholarship, emphasizing its interdisciplinary nature and the convergence of computer science, behavioral studies, and security research. These findings offer practical value for institutions and practitioners aiming to understand the intellectual structure of phishing research and guide evidence-based intervention strategies.

While the dataset was limited to Scopus-indexed publications and excluded pre-2005 research, the analysis nonetheless provides a reliable and comprehensive overview. Future research could expand to include additional databases, non-English publications, or qualitative dimensions such as discourse and genre analysis. Additionally, deeper inquiry into underrepresented regions and lesser-cited but innovative contributions may yield further insight. Overall, this bibliometric analysis underscores the utility of systematic mapping in revealing knowledge structures, tracing thematic evolution, and informing future research pathways in phishing-related cybersecurity studies.

Acknowledgements

The authors gratefully acknowledge Universiti Teknologi MARA Cawangan Perlis and Universiti Malaysia Perlis for their support and resources provided throughout the course of this research. Gratitude is also extended to the organizer, Iman Excellence and mentors of the bibliometric analysis workshop, whose guidance was vital to the completion of this study.

References

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, *11*(3). https://doi.org/10.1177/21582440211031879

Akerlof, G. A., & Shiller, R. J. (2015). Phishing for phools: The economics of manipulation and deception. In *Phishing for Phools: The Economics of Manipulation and Deception*. Princeton University Press. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84977110651&partnerID=40&md5=5b22f1e6e6596b7b42e9ccaaf1247313

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002
Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers and Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021a). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. In *Frontiers in Computer Science* (Vol. 3). Frontiers Media S.A. https://doi.org/10.3389/fcomp.2021.563060

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021b). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. In *Frontiers in Computer Science* (Vol. 3). Frontiers Media S.A. https://doi.org/10.3389/fcomp.2021.563060

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021c). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(March), 1–23. https://doi.org/10.3389/fcomp.2021.563060

Al-Khoury, A., Hussein, S. A., Abdulwhab, M., Aljuboori, Z. M., Haddad, H., Ali, M. A., Abed, I. A., & Flayyih, H. H. (2022). Intellectual Capital History and Trends: A Bibliometric Analysis Using Scopus Database. *Sustainability (Switzerland)*, *14*(18). https://doi.org/10.3390/su141811615

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Alves, J. L., Borges, I. B., & De Nadae, J. (2021). Sustainability in complex projects of civil construction: Bibliometric and bibliographic review. *Gestao e Producao*, *28*(4). https://doi.org/10.1590/1806-9649-2020v28e5389

Appio, F. P., Cesaroni, F., & Di Minin, A. (2014). Visualizing the structure and bridges of the intellectual property management and strategy literature: a document co-citation analysis. *Scientometrics*, *101*(1), 623–661. https://doi.org/10.1007/s11192-014-1329-0

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Assyakur, D. S., & Rosa, E. M. (2022). Spiritual Leadership in Healthcare: A Bibliometric Analysis. *Jurnal Aisyah : Jurnal Ilmu Kesehatan*, *7*(2). https://doi.org/10.30604/jika.v7i2.914

Barreiro Herrera, D. A., & Camargo Mendoza, J. E. (2022). A Systematic Review on Phishing Detection: A Perspective Beyond a High Accuracy in Phishing Detection. In H. Florez & H. Gomez (Eds.), *Communications in Computer and Information Science: Vol. 1643 CCIS* (pp. 173–188). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-19647-8_13

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

Chien, A., & Khethavath, P. (2023). Email Feature Classification and Analysis of Phishing Email Detection Using Machine Learning Techniques. *Proceedings of the 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2023*. https://doi.org/10.1109/CSDE59766.2023.10487729

Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S. C., & Tiong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, *484*, 153–166. https://doi.org/10.1016/j.ins.2019.01.064

di Stefano, G., Peteraf, M., & Veronay, G. (2010). Dynamic capabilities deconstructed: A bibliographic investigation into the origins, development, and future directions of the

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 40 (September 2025) PP. 19-33
DOI: 10.35631/JISTM.1040002

research domain. *Industrial and Corporate Change*, *19*(4), 1187–1204. https://doi.org/10.1093/icc/dtq027

Dodge Jr., R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security*, *26*(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

Fahimnia, B., Sarkis, J., & Davarzani, H. (2015). Green supply chain management: A review and bibliometric analysis. In *International Journal of Production Economics* (Vol. 162, pp. 101–114). https://doi.org/10.1016/j.ijpe.2015.01.003

Gu, D., Li, T., Wang, X., Yang, X., & Yu, Z. (2019). Visualizing the intellectual structure and evolution of electronic health and telemedicine research. *International Journal of Medical Informatics*, *130*. https://doi.org/10.1016/j.ijmedinf.2019.08.007

Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103158

Khiste, G. P., & Paithankar, R. R. (2017). Analysis of Bibliometric term in Scopus. *International Research Journal*, *01*(32), 78–83.

Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior*, *158*. https://doi.org/10.1016/j.chb.2024.108274

van Eck, N. J., & Waltman, L. (2007). Bibliometric mapping of the computational intelligence field. *International Journal of Uncertainty, Fuzziness and Knowldege-Based Systems*, *15*(5), 625–645. https://doi.org/10.1142/S0218488507004911

van Eck, N. J., & Waltman, L. (2010a). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

van Eck, N. J., & Waltman, L. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. *Scientometrics*, *111*(2), 1053–1070. https://doi.org/10.1007/s11192-017-2300-7

Verbeek, A., Debackere, K., Luwel, M., & Zimmermann, E. (2002). Measuring progress and evolution in science and technology - I: The multiple uses of bibliometric indicators. *International Journal of Management Reviews*, *4*(2), 179–211. https://doi.org/10.1111/1468-2370.00083

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273–303. https://doi.org/10.2753/MIS0742-1222270111

Wu, Y. C. J., & Wu, T. (2017). A decade of entrepreneurship education in the Asia Pacific for future directions in theory and practice. In Management Decision (Vol. 55, Issue 7, pp. 1333–1350). https://doi.org/10.1108/MD-05-2017-0518