DOI: 10.26354/bb.9.4.101.2025

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Bibliometric Analysis of Phishing

Abstract

Purpose: This article presents a comprehensive bibliometric analysis of scientific literature on phishing with particular emphasis on the banking and financial sector, aiming to identify key research trends, influential authors, and prospective development directions in the period 2003–2024.

Methodology: The study employs the bibliometrix tool and Web of Science database data comprising 4,245 documents from 2,355 sources. The analysis is characterized by an annual publication growth rate of 16.35% with an average of 13.73 citations per document. The corpus contains publications by 11,755 authors with 91,018 references, reflecting the multidisciplinary nature of the research field.

Results: IEEE Access dominates with 135 publications, while Computers & Security ranks second with 104 publications. Carnegie Mellon University leads among institutions with 75 publications. The analysis reveals evolution from traditional defense methods (2006–2015) toward artificial intelligence and blockchain technologies (2020–2024). The most frequently cited publications are works by Jagatic et al. (2007) – 540 citations and Anderson (2006) – 385 citations. Identification of two main thematic clusters indicates a dichotomy between security research and detection methods based on modeling.

Conclusions: Phishing research in the financial sector is characterized by intensive development with a paradigm shift toward personalized detection systems utilizing machine learning. Future directions include interdisciplinary research combining technical with behavioral aspects and application of blockchain technology in identity verification systems.

Keywords: phishing, cybersecurity, banking sector, bibliometric analysis, machine learning, learningblockchain, financial security

JEL Codes: G21, G28, O33, C80

* Patryk Król – Poznań University of Economics and Busines.

Introduction

Phishing, as a form of cybercrime, poses one of the most serious threats to the modern digital economy, including the financial sector and especially the banking sector (Zhuo et al. 2023). Phishing attacks, which use social engineering techniques to obtain confidential information such as credentials or financial information, are becoming increasingly sophisticated and pose a significant challenge to the security of financial institutions (Yuspin et al. 2024; Mwavali 2024).

In recent years, there has been a sharp increase in both the number of phishing attacks and their technological sophistication, which has prompted countermeasures by institutions responsible for electronic commerce security and researchers investigating this issue (Do et al. 2022). According to Villanueva et al. (2024), phishing attacks have increased by 46% since 2018, and the financial sector suffers an average annual loss of $3.66 million (Villanueva, Sebastian, Dextre 2024). Statistics indicate that approximately 1.2% of all emails received are phishing attempts, which translates to 3.4 billion phishing emails per day, with an estimated one in 4,200 emails constituting a phishing attempt (Bhatt et al. 2024).

Due to the high value of electronic transactions, the financial sector is particularly vulnerable to the effects of phishing attacks (Nwafor et al. 2024). Financial institutions must contend not only with traditional forms of phishing, but also with new forms such as spear phishing, vishing and attacks using artificial intelligence (Król 2024). The growth of electronic communication since the COVID-19 pandemic has further intensified these threats, contributing to an almost twofold increase in cyberattacks against financial institutions (Abdajabar and Idbeaa 2024).

Bibliometric analysis has recently become a popular tool for analysing the scope and structure of scientific research in a given field (Donthu et al. 2021). In the context of phishing research, this type of analysis allows for systematic mapping of research, identification of emerging trends, popular authors and institutions. Methodological analysis of such results allows for the identification of gaps in existing knowledge (Mutlutürk et al. 2024). Such bibliometric analyses are also used to study phishing in the financial sector. The results of these analyses make it easier to determine both what has already been researched and to identify challenges related to phishing in this sector.

Previous bibliometric studies in the field of cybersecurity have focused mainly on general aspects of threats (Perwej et al. 2021). However, relatively little attention has been paid to a detailed analysis of the literature on phishing in the financial sector. Recent analyses indicate a growing interest among researchers in the psychological factors influencing vulnerability to phishing, aspects of electronic communication security, and the integration of technological solutions with human behaviour (Mutluturk and Metin 2023). In addition, the use of artificial intelligence in detecting and counteracting phishing attacks is becoming increasingly important (Olowu et al. 2024).

The aim of this article is to conduct a bibliometric analysis of scientific literature on phishing, with a particular focus on the financial sector. The analysis includes identifying key research trends, mapping international and inter-institutional cooperation, determining the most popular publications and authors, and indicating promising directions for future research. The use of advanced bibliometric techniques allows for the development of a comprehensive picture of the state of knowledge in this field and the identification of areas requiring further scientific research. The originality of the study lies in focusing the literature analysis on the financial sector, whereas previous bibliometric analyses of phishing have mostly concentrated on general aspects of cybersecurity.

Research methodology and quantitative characteristics of the analysed publications

The study used the bibliometrix (Aria and Cuccurullo 2017) and data from the Web of Science Core Collection database, covering 4,245 documents from 2003–2024, originating from 2,355 sources. The search phrase was "phishing". This allowed for an interdisciplinary cross-section of studies on the subject to be included. The most frequently cited publications on economics and finance are discussed in a separate section. The database created reflects the dynamic growth of publications with an annual rate of 16.35%, which indicates the intensive development of the discipline under study. The average age of the publications studied is 6.45 years, with a total number of references of 91,018 and an average number of citations per document of 13.73, which can be interpreted as a significant impact of the publications on the scientific community.

An analysis of the content of the documents reveals a wealth of scientific terminology, with 1,349 keywords (Keywords Plus) and 7,975 author's keywords (Author's Keywords) identified. This terminological diversity reflects, among other things, the multidisciplinary nature of the publications studied and, indirectly, the complexity of the issues addressed.

The analysis covered publications by 11,755 authors, of whom only 284 were single authors, which indicates a high level of collaboration between authors. The average number of co-authors per document is 3.71. The level of internationalisation of collaboration in the analysed documents reaches approximately 21%.

The analysed collection of publications is dominated by conference materials (2,252 documents, i.e. 53.1% of all documents), followed by scientific articles (1,735, i.e. 40.9% of all records) (corpus). Other publications include literature reviews (94 documents), book reviews (17), editorial materials (26) and a few other items. The structure of the analysed collection of documents reflects the general structure of publications in contemporary science, with conference communication playing a key role in the popularisation of research results.

Results of the publication analysis

Table 1 illustrates the number of scientific publications on phishing according to ten scientific journals on phishing, constituting a key element of bibliometric analysis in this research area.

Table 1. Scientific journals with the highest number of publications on phishing indexed in the WoS database

No.	Journal	Number of publications
1	IEEE Access	135
2.	Computers and Security	104
3.	International Journal of Advanced Computer Science and Applications	51
4.	Electronics	41
5.	Applied Sciences-Basel	34
6.	Expert Systems with Applications	30
7.	International Journal of Computer Science and Network Security	27
8.	Information and Computer Security	22
9.	Security and Communication Networks	22
10.	CMC-Computers Materials and Continua	21

Source: own study, based on data from the WoS database, prepared using the Bibliometrix tool.

Table 2 presents a list of the most active authors of scientific publications on phishing, taking into account the total number of scientific papers. The data allows us to identify key scientists shaping the landscape of phishing research and the scale of their scientific contribution.

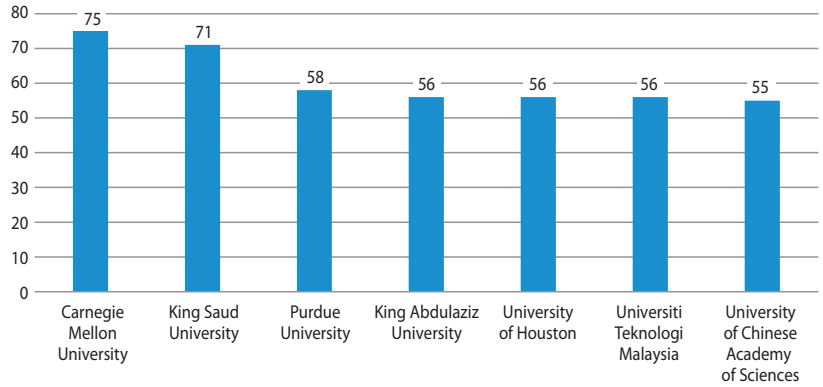
Chart 1 shows the number of scientific publications on phishing by author affiliation in seven academic institutions. Carnegie Melon University is in the lead, ahead of King Saud University by four publications. The other five institutions have a similar number of publications, ranging from 58 to 55. It is worth noting that the University of the Chinese Academy of Sciences has 55 publications. The data in Chart 1 indicate the global nature of research and publications on phishing.

Table 2. Authors with the highest number of publications on phishing indexed in the WoS database

No.	Author	Number of articles
1	Jain Ankit Kumar	17
2	Thabtah Fadi	17
3	Rao Routhu Srinivasa	15
4	Volkamer Melanie	15
5	Moore Tyler	14
6	Varshney Gaurav	14
7	Allodi Luca	13
8	Chiba Daiki	13
9	Chiew Kang Leng	13
10	Jourdan Guy-Vincent	13
11	Verma Rakesh M	13
12	Vishwanath Arun	13
13	Wu Jiajing	13

Source: own study, based on data from the WoS database, prepared using the Bibliometrix tool.

Figure 1. Author affiliations by number of publications on phishing indexed in the WoS database



Source: own work, based on data from the WoS database, compiled using the Bibliometrix tool.

An analysis of the most frequently cited publications in the field of phishing research reveals key works that have shaped the contemporary understanding of this phenomenon. Table 3 presents the 10 most frequently cited publications in the general collection of literature on phishing, without distinction by subject category.

Table 3. Authors with the most frequently cited publications on phishing indexed in the WoS database

Author and year of publication	Journal/Conference	Citations Total	Citations per year	Normalised citations[a)]
Jagatic et al. (2007)	Communications of the ACM	540	28.42	16.63
Anderson and Moore (2006)	Science	385	19.25	17.25
Sheng et al. (2010)	CHI Conference Proceedings	366	22.88	10.67
Xiang et al. (2011)	ACM Transactions on Information and System Security	321	21.40	11.05
Sahingoz et al. (2019)	Expert Systems with Applications	319	45.57	17.67
Krombholz et al. (2015)	Journal of Information Security and Applications	291	26.45	19.54
Khonji et al. (2013)	IEEE Communications Surveys and Tutorials	266	20.46	16.64
Hong (2012)	Communications of the ACM	264	18.86	12.33
Grier et al. (2010)	ACM Conference on Computer and Communications Security	261	16.31	7.61
Egelman et al. (2008)	CHI Conference Proceedings	259	14.39	17.13

[a)] Normalised citations are a measure that takes into account the age of a publication and the average number of citations in a given year, calculated as the number of citations divided by the average number of citations for publications from the same year. A value above 1 indicates an above-average impact of the publication.

Source: own study, based on data from the WoS database, prepared using the Bibliometrix tool.

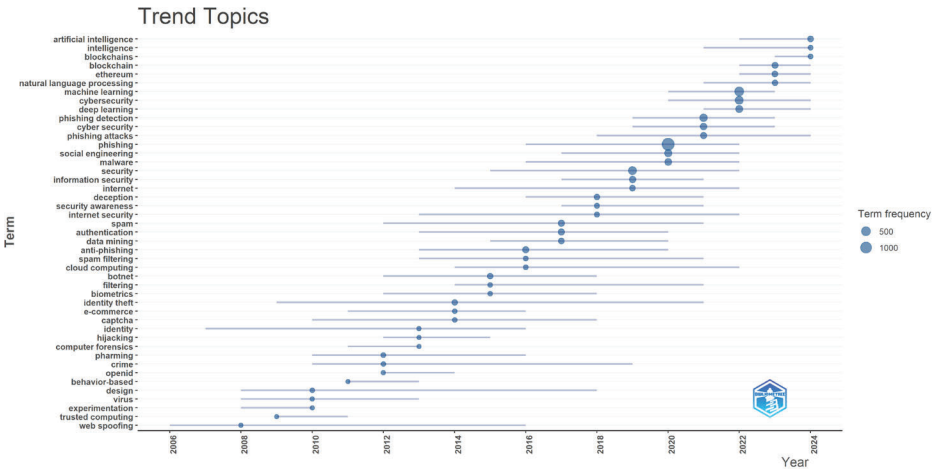
Jagatic et al. (2007) initiated research on social phishing in their groundbreaking article published in *Communications of the ACM*. It concerned the concept of using social networks in phishing attacks and laid the foundations for determining the role of social factors in the vulnerability of people using these networks to attacks. Anderson and Moore (2006) presented fundamental analyses of security economics in the prestigious journal *Science*, which became the basis for subsequent research on the economic aspects of cybercrime. This work, with 385 citations in WoS and over 1,100 citations in Google Scholar, influenced the development of an interdisciplinary approach to phishing research, combining technical and economic aspects. Sheng et al. (2010) presented significant research on the factors influencing users' vulnerability to phishing in the CHI conference proceedings, achieving 366 citations. Their research contributed to a better understanding of the psychological patterns exploited by cybercriminals. Xiang et al. (2011) presented an innovative approach to phishing detection in *ACM Transactions on Information and System Security*, which has 321 citations. Their methodology became the basis for many subsequent phishing attack detection systems. Also significant is the work of Sahingoz et al. (2019) published in *Expert Systems with Applications*, which has already reached 319 citations and the highest number of citations per year (45.57). This publication focuses on the use of artificial intelligence in phishing detection. Krombholz et al. (2015) in *the Journal of Information Security and Applications* conducted a comprehensive analysis of social engineering attacks, which has been cited 291 times. Their research has contributed to a better understanding of both the psychological aspects of phishing and the manipulation mechanisms used by attackers. Khonji et al. (2013) published an important literature review on phishing in *IEEE Communications Surveys and Tutorials*, which has been cited 266 times, systematising previous research and identifying directions for future research.

Chart 2 contains a set of concepts used in phishing research between 2006 and 2024, illustrating the transition from early technical issues such as web spoofing and trusted computing (2006–2009), through the development of detection methods based on Bayesian classification and behavioural analysis (2010–2015), to the application of machine learning, artificial intelligence, and blockchain technology (2020–2024). The most frequently occurring term is „phishing" (1326 occurrences), followed by „machine learning" (495 occurrences) and „security" (436 occurrences). Figure 2 symbolically illustrates the transformation of the research paradigm from traditional rule-based and filter-based defence methods (spam filtering, anti-phishing) in 2013–2016 towards advanced methods of artificial intelligence, natural language processing and deep learning in recent years (2021–2024), which means, among other things, the growing importance of automation and intelligent systems in the fight against phishing. Particularly noticeable is the increase in interest in blockchain and Ethereum technologies since 2022, suggesting the adaptation of new approaches to cyber security in the context of decentralised financial systems.

It is worth noting that the most productive authors (Table 2) do not coincide with the authors of the most cited publications (Table 3). There may be several reasons for this phenomenon. First, the authors of the most frequently cited works often

published during the pioneering period of research (2006–2015), laying the foundations of the field, while the most productive authors are active in later years, developing existing concepts. Second, groundbreaking publications may have a greater impact than many incremental works. Third, this difference may reflect thematic specialisation – the most productive authors may focus on narrow technical aspects, while the most cited works are interdisciplinary or review-oriented.

Figure 2. Thematic trends in phishing research, 2006–2024, by keyword



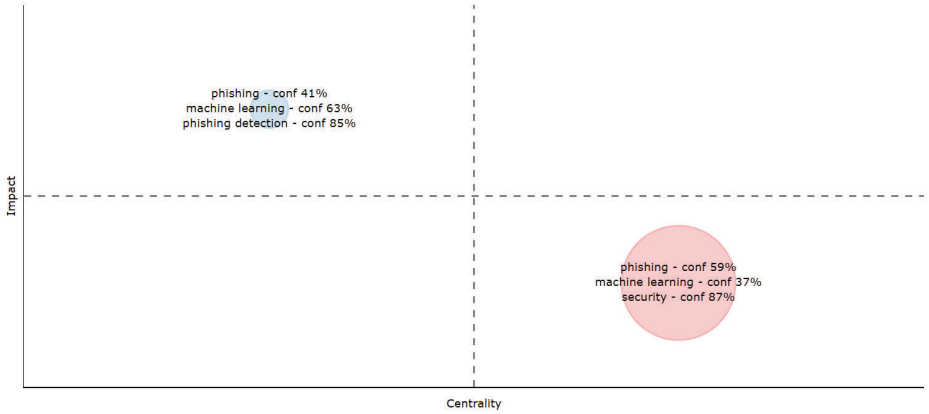
Legend: The size of the circles reflects the number of publications containing a given keyword in a given year, and the horizontal lines show the period of occurrence of the topic in the analysed literature.

Source: own study, based on data from the WoS database, prepared using the Bibliometrix tool.

Chart 3 contains thematic clusters (according to Keywords Plus) created on the basis of an analysis of literature on phishing and their interconnection through common citations. This resulted in two research clusters with different levels of centrality and influence. Cluster 1 (pink), created on the basis of 137 documents, focuses on the issues of „security", „attacks" and „classification" with confidence levels of 79.2%, 62.5% and 59.1%, respectively, achieving a centrality of 0.401 and a local impact of 7.542. These parameters indicate its fundamental role in research on security and the classification of phishing attacks. Cluster 2 (blue), created on the basis of 113 documents, focuses research on „features," „model" and „websites" with higher confidence levels (88.9%, 57.1%, 86.7%) and slightly higher centrality (0.399) as well as greater local influence (8.411). This indicates a focus on modelling and analysing the technical features of websites. The division of the studied documents into two clusters indicates a dichotomy in phishing research. Namely, an approach focused on the analysis of security threats and an approach focused on technical detection methods based on features and modelling. The

second cluster has a stronger influence on the development of research in this area, despite the smaller number of publications. This is most likely due to the higher level of innovation and citations in research on phishing detection algorithms.

Figure 3. Thematic clusters related to phishing



Source: own study, based on data from the WoS database, prepared using the Bibliometrix tool.

Characteristics of the most frequently cited publications on phishing in economics and finance

Phishing, as a form of cybercrime, has a significant impact on financial security and even the stability of the banking sector. This thesis is justified primarily by the estimated losses amounting to billions of dollars annually, as well as the undermining of consumer confidence in financial services and trading in electronic distribution channels. Unlike the publications in Table 3, the following overview includes the 10 most frequently cited publications from the WoS database in the „Economy & Business Finance" category only, which allows for an in-depth analysis of the economic and financial consequences of phishing for the banking sector.

Herley and Florêncio (2010) in their paper „Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy" analysed the illegal cyber economy, focusing in particular on IRC markets[1] offering stolen identities,

[1] The IRC market does not exist as a financial or commercial market in the classical sense. IRC is primarily a communication technology (Internet Relay Chat), i.e. a network of online chat channels. There are various IRC networks in Poland, e.g. PIRC.PL, which can be called a "market" in the social sense as a place and means of exchanging information, contacts and services. It operates in a client-server architecture: the user connects to the IRC server using a client programme, and conversations take place on thematic channels. Channels can be public (open to everyone) or private (for invited users only).

phishing kits, botnets[2] and cybercrime-related services. The authors demonstrated the existence of sophisticated 'underground' markets characterised by a high level of specialisation and maturity, with a comprehensive division of labour and range of services, which revolutionised the understanding of the economic aspects of cybercrime. This work has been cited 62 times and has been instrumental in understanding the economic mechanisms driving phishing attacks. Hornuf et al. (2022), in their study "Initial coin offerings, information disclosure, and fraud" published in *Small Business Economics*, conducted a comprehensive analysis of fraud in Initial Coin Offerings (ICOs), documenting various types of fraud and showing that fraudulent ICOs are on average significantly larger than the average for other types of fraud. The authors discovered a paradox whereby issuers who disclose their code on GitHub[3] are more vulnerable to phishing and hacking attacks, pointing to the risks of transparency. This publication, cited 54 times, has made a key contribution to understanding the relationship between information disclosure and vulnerability to cybercrime in the financial sector.

Shkarlet et al. (2018) in their paper „Determinants of the Financial Services Market Functioning in the Era of the Informational Economy Development" published in *the Baltic Journal of Economic Studies* identified the determinants of the functioning of the financial services market in the era of the development of the information economy. The authors demonstrated objective links between financial systems and the national economy, emphasising the transformative impact of information technology on the functioning of financial institutions. This publication, cited 17 times, provided a theoretical framework for understanding the impact of digitalisation on the security of the financial sector.

Bayl-Smith et al. (2020), in their study „Cue Utilisation, Phishing Feature and Phishing Email Detection" presented *at the 24th International Conference on Financial Cryptography and Data Security*, developed the concept of cues as a unique predictor of phishing feature detection. The study, conducted on 127 psychology students, demonstrated the importance of cognitive processes in identifying phishing emails. This work, cited 12 times, contributed to a better understanding of the psychological mechanisms of phishing vulnerability in a financial context.

O'Leary (2019), in his article „What Phishing Emails Reveal: An Exploratory Analysis of Phishing Attempts Using Text Analysis" published in *the Journal of Information Systems*, conducted a textual analysis of phishing emails targeting accountants and auditing firms. By comparing a database of phishing messages with Enron emails, the author demonstrated statistically significant differences in many categories of text variables. This publication, cited 11 times, generated a phishing model as

[2] Botnets are networks of devices (computers, smartphones, servers or IoT equipment) infected with malware that are remotely controlled by cybercriminals. Each device in such a network acts as a "bot" and executes the operator's commands without the owner's knowledge.

[3] GitHub is the world's largest platform for code collaboration, based on the Git version control system. It allows developers to store projects, track changes, collaborate as a team, and publish software in an open source or private model.

"power" based on the variables: friend, achievement, money, and work, which became the basis for subsequent research on text analysis in a financial context.

Bakarich and Baranek (2020) in their case study „Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise" published in *Current Issues in Auditing* analysed the case of a US public company that fell victim to a scam called Business Email Compromise (BEC), as a result of which an employee unintentionally transferred millions of dollars to fraudulent accounts. This publication, cited 8 times, provided valuable educational insights for the auditing and financial sectors on the growing prevalence and scale of this type of corporate fraud.

Das et al. (2020) in their paper „User-Centered Risk Communication for Safer Browsing" presented at *the 24th International Conference on Financial Cryptography and Data Security* developed a risk management tool combining personalised blocking, filtering and alerts into a single holistic system. The authors used simple metaphorical illustrations that functioned both as risk communication and browser settings controls. This publication, cited 7 times, made a significant contribution to the development of a user-centred approach to online financial security.

Taylor-Jackson et al. (2020), in their paper „Incorporating Psychology into Cyber Security Education: A Pedagogical Approach" presented at *the 24th International Conference on Financial Cryptography and Data Security*, emphasised the role of the human factor in cyber security. The authors demonstrated that many cybersecurity incidents involve persuading deliberately selected individuals to perform specific behaviours or actions, such as opening a link in a phishing email. This publication, cited 7 times, contributed to the development of pedagogical approaches that incorporate psychology into financial cybersecurity education.

Basu (2018), in his paper „Markets and Manipulation: Time for a Paradigm Shift?" published in *the Journal of Economic Literature*, presented an overview of the growing importance in economics of human emotional weaknesses, attachment to social norms, and systematic irrationalities that influence market decision-making. The author emphasised that human beings are susceptible to manipulation by unscrupulous agents marketing their services or goods. This publication, cited six times, provided a cognitive framework for understanding the psychological basis of vulnerability to financial fraud.

Olifer et al. (2017), in their study „Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs" published in *Technological and Economic Development of Economy*, analysed the costs of implementing information security standards. The authors showed that, according to a PricewaterhouseCoopers analysis, the average cost of a single information security and data protection breach doubled in 2015, and the number of organisations reporting serious breaches increased from 9% in 2015 to 17% in 2016. This publication, cited 6 times, provided fundamental economic data on the costs of cybercrime to the financial sector.

Conclusion

A bibliometric analysis of scientific literature on phishing, with particular emphasis on the financial sector, characterises the state of research on this phenomenon and indicates the main trends and directions of development. The dynamics of research interest in phishing, reflected in an annual publication growth rate of 16.35%, confirms the growing threat it poses to the cyber security of financial institutions and the urgent need for systematic scientific research (Donthu et al. 2021).

The evolution of phishing research paradigms between 2003 and 2024 indicates a shift from traditional approaches based on technical analysis and rules towards advanced methods using artificial intelligence, machine learning and natural language processing. Since 2022, there has been a noticeable surge of interest in blockchain and Ethereum technologies, signalling the exploration of new security mechanisms in the context of decentralised financial systems (Sahingoz et al. 2019; Das et al. 2020). The publication of numerous articles in this field in prestigious journals such as IEEE Access (135 publications) and Computers & Security (104 publications) indicates the existence of recognised publishing platforms in the field of phishing research. The dominance of open access publications reflects the trend in disseminating cybersecurity research results. At the same time, the global nature of research collaboration represented by leading institutions in North America, Asia and the Middle East highlights the universal nature of phishing threats and the need for international coordination of research activities.

An analysis of thematic clusters reveals a clear dichotomy between research focused on security threat analysis and technical detection methods based on features and modelling, with the latter cluster having a stronger influence on the development of the field, suggesting greater innovation in the area of phishing detection algorithms.

A review of the most frequently cited publications on phishing from an economic and financial perspective points to the fundamental importance of Herley and Florêncio's (2010) work on the economics of the underground cyber economy and the growing importance of research on ICOs and cryptocurrencies in the context of financial fraud (Hornuf et al. 2022). The identification of research gaps points to the need to intensify research in several key areas. First, interdisciplinary research combining technical and behavioural aspects is needed, taking into account the specific characteristics of financial service users and the cultural determinants of vulnerability to phishing. Second, there is a need for more in-depth analysis of the long-term economic effects of phishing attacks on the stability of the banking sector and the effectiveness of various cybersecurity investment strategies. Third, research is needed on the ethics of using artificial intelligence in phishing detection, particularly in the context of protecting the privacy of financial institution customers.

Future research should focus on the development of personalised phishing detection systems using advanced machine learning algorithms tailored to the specific risk profiles of banking service users. Research on the use of blockchain technology in

the creation of decentralised identity verification systems and the use of natural language processing for real-time semantic analysis of phishing communications seems particularly promising. The practical implications of the analysis indicate the need for an integrated approach to cybersecurity in financial institutions, combining advanced technological solutions with systematic user education and regular organisational vulnerability assessments. Recommendations for practitioners include investing in multi-layered defence systems, developing organisational security cultures, and creating mechanisms for international cooperation in the exchange of threat information.

This bibliometric analysis confirms that research on phishing in the financial sector is undergoing rapid development, characterised by increasing methodological sophistication and the integration of various scientific disciplines. The future of this field is likely to be shaped by advances in artificial intelligence, the development of blockchain technology, and the growing importance of behavioural factors in the design of cybersecurity systems, which requires continued systematic research and close cooperation between academia and financial sector practitioners.

Bibliography

Abdajabar A., Idbeaa T. (2024). Cybercrime's Threat to Financial Institutions During COVID-19. *AlQalam Journal of Medical and Applied Sciences*, 46–52.

Anderson R. Moore T. (2006). The economics of information security. *Science*, 314(5799), 610–613.

Aria M., Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975.

Bakarich K.M., Baranek D. (2020). Something phish-y is going on here: A teaching case on business email compromise. *Current Issues in Auditing*, 14(1), A1–A9. https://doi.org/10.2308/ciia-52706

Basu K. (2018). Markets and manipulation: Time for a paradigm shift? *Journal of Economic Literature*, 56(1), 185–205. https://doi.org/10.1257/jel.20161410

Bayl-Smith P., Sturman D., Wiggins M. (2020). Cue utilization, phishing feature and phishing email detection. W *Financial Cryptography and Data Security, FC 2020* (pp. 56–70). Springer. https://doi.org/10.1007/978-3-030-54455-3_5

Bhatt P., Obaidat M.S., Dangwal G., Das A.K., Wazid M., Sadoun B. (2024). Machine learning-based security mechanism for detecting phishing attacks. In *2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)* (pp. 1–6). IEEE. https://doi.org/10.1109/CCCI61916.2024.10736460

Das S., Abbot, J., Gopavaram S., Blythe J., Camp L.J. (2020). User-centered risk communication for safer browsing. In *International conference on financial cryptography and data security* (pp. 18–35). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_2

Do N.Q., Selamat A., Krejcar O., Herrera-Viedma E., Fujita H. (2022). Deep learning for phishing detection: Taxonomy, current challenges and future directions. *Ieee Access*, *10*, 36429–36463. https://doi.org/10.1109/ACCESS.2022.3151903

Donthu N., Kumar S., Mukherjee D., Pandey N., Lim, W.M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of business research*, *133*, 285–296.

Egelman S., Cranor L.F., Hong J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065–1074.

Grier C., Ballard L., Caballero J., Chachra N., Dietrich C.J., Levchenko K., …, Voelker G.M. (2010). Manufacturing compromise: The emergence of exploit-as-a-service. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 821–832. https://doi.org/10.1145/1866307.1866311

Herley C., Florêncio D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In *Economics of Information Security and Privacy* (pp. 33–53). Springer. https://doi.org/10.1007/978-1-4419-6967-5_3

Hong J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

Hornuf L., Kück T., Schwienbacher A. (2022). Initial coin offerings, information disclosure, and fraud. *Small Business Economics*, 58(4), 1741–1759. https://doi.org/10.1007/s11187-021-00471-y

Jagatic T.N., Johnson N.A., Jakobsson M., Menczer F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

Khonji M., Iraqi Y., Jones A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys i Tutorials*, 15(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Król P. (2024). Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej. *Bezpieczny Bank*, 94(1), 25–42. https://doi.org/10.26354/bb.2.1.94.2024

Krombholz K., Hobel H., Huber M., Weippl E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Mutlutürk M., Metin B. (2023). Mapping The Phishing Attacks Research Landscape: A Bibliometric Analysis And Taxonomy. *J. Theor. Appl. Inf. Technol*, *101*, 6758–6780.

Mutlutürk, M., Wynn, M. i Metin, B. (2024). Phishing and the Human Factor: Insights from a Bibliometric Analysis. *Information*, 15(10), 643. https://doi.org/10.3390/info15100643

Mwavali, A. (2024). Combating phishing in Kenya: A supervised learning model for enhanced email security in Kenyan financial institutions. *International Journal of Technology and Systems*, 9(4), 23–36.

Nwafor K.C., Ikudabo A.O., Onyeje C.C., Ihenacho D.O.T. (2024). Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive*, 13(01), 2895–2910.

O'Leary, D.E. (2019). What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis. *Journal of Information Systems*, 33(3), 285–307. https://doi.org/10.2308/isys-52481

Olifer D., Goranin N., Kaceniauskas A., Cenys A. (2017). Controls-based approach for evaluation of information security standards implementation costs. *Technological and Economic Development of Economy*, 23(1), 196–219. https://doi.org/10.3846/20294913.2017.1280558

Olowu O., Adeleye A.O., Omokanye A.O., Ajayi A.M., Adepoju A.O., Omole O.M., Chianumba E.C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *Advanced Research and Review*, 21(2), 227–237.

Perwej Y., Abbas S.Q., Dixit J.P., Akhtar N., Jaiswal A.K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, 9(12), 669–710.

Sahingoz O.K., Buber E., Demir O., Diri B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Sheng S., Holbrook M., Kumaraguru P., Cranor L.F., Downs J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382.

Shkarlet S., Dubyna M., Zhuk O. (2018). Determinants of the financial services market functioning in the era of the informational economy development. *Baltic Journal of Economic Studies*, 4(3), 349–357. https://doi.org/10.30525/2256-0742/2018-4-3-349-357

Taylor-Jackson J., McAlaney J., Ashenden D., Dale J. (2020). Incorporating psychology into cyber security education: A pedagogical approach. In *Financial Cryptography and Data Security, FC 2020* (pp. 207–217). Springer. https://doi.org/10.1007/978-3-030-54455-3_15

Villanueva J., Sebastian J. Dextre J. (2024, July). Web Portal Validation Model by Digital Signature and ISO 27002 to Reduce Private Credentials Theft for Phishing Attacks to Financial Sector Customers. In *2024 International Conference on Electrical, Computer and Energy Technologies ICECET* (pp. 1–5). IEEE.

Xiang G., Hong J., Rose C.P., Cranor L. (2011). CANTINA+: A feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security*, 14(2), 1–28. https://doi.org/10.1145/2019599.2019606

Yuspin W., Putri A.O., Fauzie A., Pitaksantayothin J. (2024). Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities.*International Journal of Safety & Security Engineering*, 14(6).

Zhuo S., Biddle R., Koh Y.S., Lottridge D. Russello G. (2023). SoK: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security*, 26(3), 1–27.