Computers & Security 132 (2023) 103387

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Mitigation strategies against the phishing attacks: A systematic literature review

Bilal Naqvi[a], Kseniia Perova[a], Ali Farooq[b,c], Imran Makhdoom[d], Shola Oyedeji[a], Jari Porras[a]

[a] Software Engineering, LENS, LUT University, Lappeenranta, Finland
[b] Qatar Computing Research Institute, Hamad Bin Khalifa University, Doha, Qatar
[c] Department of Computing, University of Turku, Finland
[d] National University of Sciences and Technology, Pakistan

ARTICLE INFO

Article history:
Received 31 December 2022
Revised 24 June 2023
Accepted 8 July 2023
Available online 9 July 2023

Keywords:
Guidelines and recommendations
Mitigation strategies
Phishing attacks
Systematic
Literature review

ABSTRACT

Phishing attacks are among the most prevalent attack mechanisms employed by attackers. The consequences of successful phishing include (and are not limited to) financial losses, impact on reputation, and identity theft. The paper presents a systematic literature review featuring 248 articles (from the beginning of 2018 until March 2023) across the main digital libraries to identify, (1) the existing mitigation strategies against phishing attacks, and the underlying technologies considered in the development of these strategies; (2) the most considered phishing vectors in the development of the mitigation strategies; (3) anti-phishing guidelines and recommendations for organizations and end-users respectively; and (4) gaps and open issues that exist in the state of the art. The paper advocates for the need to consider the abilities of human users during the design and development of the mitigation strategies as only technology-centric solutions will not suffice to cater to the challenges posed by phishing attacks.

© 2023 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

1. Introduction

Security incidents and breaches targeted towards exploiting the human aspects of cyber security are on the rise every passing year. The data breach investigations report (DBIR) by Verizon identifies that 82% of the analyzed breaches involved the human element (Verizon, 2022). One common attack that exploits the human aspects of cyber security is known as the phishing attack. Phishing occurs when the attacker persuades the victim into doing something which is not beneficial for the victim or the system. Phishing is a crime based on social engineering (Chen & Chen, 2019). Sameen et al., (2020) define a phishing attack as a fraudulent attempt to portray a trusted party to obtain sensitive information. It is obvious from these definitions that phishing is a deceitful attempt, yet the intent behind the attack may vary. Typically, the intent is to access financial details and steal system credentials or other sensitive information. Moreover, phishing is also used as an attack vector to execute other attacks such as ransomware attacks. More recently phishing has targeted organizations and made them suffer in terms of cost to contain malware, productivity loses, cost to contain credential compromise, and cost of ransomware from phishing, besides loss of reputation in front of their customers and competitors (Ponemon Institute, 2021). It is relevant to state that phishing appeared as the costliest attack vector in 2022 with an average cost of US Dollars 4.91 million per data breach (IBM, 2022).

Phishing can be performed over different mediums using different vectors; three mediums used commonly for phishing include (1) the Internet, (2) short messaging services, and (3) voice (Chiew et al., 2018). Within each of these mediums, different vectors are used to execute the attack. For instance, with the Internet as a medium, common phishing vectors include email, eFax, instant messaging, social networks, websites, and Wi-Fi. In the case of short messaging services and voice as mediums, Smishing and Vishing respectively are the relevant attack vectors. Recent trends show that phishing attempts have been reported across all sectors ranging from financial institutions such as banks to educational institutions, and governmental organizations to the healthcare sector (IBM, 2022).

With all its manifestations and forms phishing alone poses a serious challenge, however, the challenge becomes sterner when phishing is used as a vector to launch other attacks such as ransomware attacks. Considering the increasing trends and dire consequences of phishing attacks both as an attack and as an attack vector, the objectives of this paper are: (1) to identify the existing mitigation strategies against phishing attacks, (2) to identify the

E-mail address: syed.naqvi@lut.fi (B. Naqvi).

https://doi.org/10.1016/j.cose.2023.103387
0167-4048/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

phishing vectors mostly considered in the developed of the proposed mitigation strategies, (3) to synthesize anti-phishing guidelines and recommendations for organizations and end-users respectively, and (4) to identify the gaps and open issues that exist in the state of the art. While considering these objectives, a systematic literature review (SLR) was conducted to find answers to the following research questions:

- **RQ-1:** What mitigation strategies against phishing attacks have been proposed in the existing literature?
- **RQ-2:** Which phishing vectors have been mostly considered in the development of mitigation strategies?
- **RQ-3:** What anti-phishing guidelines and recommendations (for organizations and end-users) can be synthesized from the existing literature?
- **RQ-4:** What gaps and open issues emerge from the analysis of the existing literature?

The guidelines for conducting SLR proposed by Kitchenham et al., (2009) were followed in this paper. While complying with the criteria set in line with the guidelines for SLR, 248 articles were included in this study. Briefly, the results of the study show that the mitigation strategies against phishing attacks can be classified mainly into three categories namely, (1) anti-phishing systems, (2) models and frameworks, and (3) human-centric mitigation strategies. Moreover, there are several underlying concepts and technologies considered in the development of these mitigation strategies including machine learning, neural networks, cryptography, and natural language processing, among others. Furthermore, the most focused phishing vector considered in the development of mitigation strategies is the website followed by email.

Contributions of the paper. The paper summarizes the state of the art concerning the mitigation strategies against phishing attacks. Main contributions include (1) analyses of the state of the art (i) to classify the existing literature in terms of the categories of the solution proposed, (ii) to identify the underlying technologies considered in the mitigation strategies, and (iii) to identify which phishing vector have been focused upon the most in the development of the mitigation strategies, (2) the paper lists 77 anti-phishing guidelines and recommendations (extracted from the existing literature) for organizations and end-users respectively, and (3) the gaps and open issues that emerge after the analysis of the state of the art have also been presented.

Structure of the paper. The remainder of the paper is organized as follows. Section 2 presents the related work. Section 3 discusses the methodology adopted for this study. Section 4 reports the results of the study, and Section 5 concludes the paper.

2. Related work

With phishing attacks emerging among the top trends of cyber-attacks, there have been efforts by the research community to mitigate the challenges posed by phishing attacks. Consequently, studies have been published on understanding the phishing phenomenon, users' responses, and mitigation techniques. A number of systematic literature reviews (SLR) have been published over the past years to synthesize the knowledge and guide future research in the topic area. A list of recent SLRs describing their focus, data sources, publication types used in the review, literature usable sample size, the time frame of the review, guidelines followed, and the main findings are presented in Table 1. It is important to note that only the papers that were explicitly mentioned as SLR by their respective authors have been considered in this Section. However, other systematization of knowledge (SOK) papers such as rapid reviews, literature reviews, or papers presented as SOKs were not considered. In our observation, most such SOKs do not have methodological rigor to be replicated in the future.

Some of the SLRs focus on the phishing phenomenon by examining the definitions (Lastdrager, 2014; Dou et al., 2017), while others examine human-factor in phishing susceptibility and countermeasures (Das et al., 2019; Desolda et al., 2021). However, several other SLRs focus on phishing detection and anti-phishing approaches (Benavides et al., 2020; Arshad et al., 2021; Catal et al., 2022; Abdillah et al., 2022; Salloum et al., 2022; Safi & Singh, 2023) while some others describe phishing attacks, including the motivation for the attacks (Das et al., 2019). Furthermore, some reviews are focused on the attack vectors such as Safi & Singh (2023) synthesis of the literature on a phishing website, Salloum et al., (2022) focused on phishing detection in emails, and Abdillah et al., (2022) discuss several attack vectors. Among the SLRs, one review (Das et al., 2019) provides a holistic picture. Overall, the available SLRs show a scarcity of reviews that holistically identify the attack vectors, mitigation techniques, and gaps that exist in the state of the art.

In addition to the topic coverage, the existing SLRs have methodological limitations too. The most recent holistic SLR (Das et al., 2019) was conducted in 2019 using a single data source (ACM digital library) without using any review guidelines. While recent SLRs such as Safi & Singh (2023), Salloum et al., 2022, and Abdillah et al., 2022 are comprehensive in terms of publication sources, type of publications, and timeframe, these are quite narrowly focused (see Table 1 for details). Therefore, this SLR addresses the gaps in the current state of the art by considering a holistic approach concerning anti-phishing mitigation strategies backed by a sound methodology and focusing on the publications over the last 5 years (i.e., from 2018 until March 2023).

3. Methodology

In line with the methodology presented by Kitchenham et al. (2009), this study was conducted in three stages: planning, conducting, and reporting. The details of the planning and conducting phase are presented in this Section, however, the reporting phase is explained in Section 4.

3.1. Planning the SLR

This phase involved the following activities, (1) formulating the research questions, (2) defining the search string, (3) selecting the databases for search, and (4) defining the inclusion and exclusion criteria.

3.1.1. Formulating the research questions

As mentioned earlier, firstly we analyzed the existing SLR papers on the topic to identify the gaps in the state of the art. These gaps were then considered while formulating the research questions considered in this SLR. The main goal of this study is to identify the mitigation strategies against phishing attacks holistically. In line with this goal, the research questions (as mentioned in Section 1) were formulated. Briefly, RQ 1 focuses on identifying the mitigation strategies that have been proposed to counter phishing attacks, it was also intended to identify how can the mitigation strategies be classified. Since several different vectors can be used for executing phishing attacks, RQ 2 focuses on identifying the most considered phishing vectors in the development of mitigation strategies. RQ 3 aims to synthesize guidelines and recommendations from the existing literature that can assist organizations and end users in mitigating phishing attacks. RQ 4 aims to present gaps and open issues which emerge based on an analysis of the existing literature.

Table 1
State of the art concerning SLRs in the domain

Source	Focus	Data sources	Publication Types	Usable Sample	Time frame	Guidelines	Main Findings
Lastdrager, 2014	Identify Phishing definitions and their characteristics in terms of assets, actors, and activities	1 ACM 2 IEEE Xplore 3 Scopus	Journal & Conference Publications	536	From: No limit To: August 2013	Kitchenham and Charters, 2007	Phishing definition
Catal et al., 2022	The review explores and analyzes the approaches, data sources, datasets, feature selection techniques, DL algorithms, evaluation parameters and validation approaches, and implementation platforms used in the machinelearning model life cycle; and reported challenges and proposed solutions.	1 ACM 2 IEEE Xplore 3 ScienceDirect 4 Scopus 5 Springer 6 Web of Science	Journal Publications	43	From: No limit To: August 2020	Kitchenham et al., 2009	Machine learning-based phishing detection techniques
Desolda et al., 2021	Discusses human factors in phishing attacks and human factors-based solutions to reduce the phishing attacks	1 ACM 2 IEEE Xplore 3 Google Scholar 4 Science Direct 5 Scopus 6 Springer 7 Nine specific conferences and journals	Journal & Conference Publications	52	From: 2001 To: May 2019	Kitchenham 2004	Human factors in phishing attacks and users-based countermeasures
Abdillah et al., 2022	Describe the most occurring phishing attack vectors, data sources, and identification methods used to mitigate the phishing attacks, and performance evaluation methods	1 ACM 2 Emerald 3 IEEE Xplore 4 Springer 5 Wiley	Journal Publications	59	From: 2010 To: 2020	Unclear	phishing attack vectors, data sources, and identification methods
Das et al., 2019	Discusses technical and individual attributes of phishing attacks, motivation for phishing attacks, and users characteristics (human factor)	1 ACM	Journal & Conference Publications	51	From: no limit To: 2019	Unclear	Technical and individual attributes of phishing attacks, motivation for phishing attacks, and human factors
Benavides et al., 2020	Describes and classifies deep learning algorithms based phishing mitigation solutions	1 ACM 2 IEEE Xplore 3 ScienceDirect 4 Springer 5 Taylor & Francis	Journal & Conference Publications	19	From: no limit To: 2020	Kitchenham et al., 2009	Machine learning-based phishing detection techniques
Dou et al. (2017)	Presents a systematic study of software-based phishing detection schemes	Unclear	Journal & Conference Publications	unclear	From: 2010 To: June 2016	Unclear	Phishing definitions, Software-based phishing detection schemes
Arshad et al., 2021	Presents a review of the literature describing phishing and anti-phishing techniques	1 ACM 2 IEEE Xplore 3 Google Scholar	Journal & Conference Publications	20	From: 2010 To: 2020	Kitchenham et al., 2009	Phishing and anti-phishing techniques

(*continued on next page*)

Table 1 (*continued*)

Source	Focus	Data sources	Publication Types	Usable Sample	Time frame	Guidelines	Main Findings
Salloum et al., 2022	Review of literature discussing natural language processing (NLP) for detecting phishing emails	1 ACM 2 Emerald 3 Google Scholar 4 IEEE Xplore 5 SAGE 6 ScienceDirect 7 Springer 8 Taylor & Francis 9 Wiley	Journal & Conference Publications	100	From: 2006 To: 2022	Kitchenham and Charters, 2007	NLP-based phishing email detection techniques
Safi & Singh, 2023	Review of literature on different phishing website detection approaches	1 ACM 2 Elsevier 3 IEEE Xplore 4 Springer 5 Other articles	Journal & Conference Publications, Thesis, Book chapters, grey literature	80	From: 2017 To: Feb 2022	Brereton et al., 2007; Kitchenham et al., 2010	Types of phishing website detection techniques (not limited to machine learning-based solutions), datasets, and comparative performance evaluation.
Current work	Presents state of the art concerning mitigation techniques against phishing holistically by not limiting it to any specific vectors.	1 ACM 2 IEEE Xplore 3 Scopus 4 Springer 5 Web of Science	Journal and Conference Publications, Book chapters	248	From: 2018 To: March 2023	Kitchenham et al., (2009), PRISMA	(i) Most focused technologies and concepts considered in the development of the mitigation strategies, (ii) Anti-phishing recommendations and guidelines from the existing literature

3.1.2. Defining the search string

Based on the research questions, keywords were identified for defining the search query. The most relevant keywords while considering the research questions included: phishing, guidelines, best practices, tools, prevention techniques, prevention, mitigation, and solutions. Therefore, the following search query was formulated:

- "Phishing" AND "guidelines OR best practices OR tools OR prevention techniques OR prevention OR mitigation OR solutions"

It is important to note that different databases and digital libraries (considered during this SLR) have their syntax for the resultant search queries. Therefore, the query above was reformatted (while retaining the meaning) across each database while performing the search. The resultant query run across each database is presented in Appendix-I.

3.1.3. Selecting the publication sources for search

Researchers have used a variety of sources for searching potentially relevant publications. These sources can be divided into databases, such as Web of Science and Scopus, digital libraries, such as ACM, IEEE, and Springer, and search engines such as Google Scholar and ScienceDirect. Among these, Web of Science, Scopus, and Google Scholar are considered the largest sources of publications (Farooq et al., 2021). However, Google Scholar has been criticized for inconsistencies, and therefore, we only considered Web of Science and Scopus owing to their better coverage (Adriaanse & Rensleigh, 2013; Falagas et al., 2008). Moreover, Google Scholar does not provide the functionality to search in title, abstract, and keywords resulting in a large number of irrelevant publications. Furthermore, we included three digital libraries, ACM digital library, IEEE Xplore, and Springer being comprehensive data sources in computing (Valente et al., 2022). In this way, we not only included the largest sources for publications but also identified multiple sources of publication, which is in line with Kitchenham et al., (2009). The final list of publication sources considered in this SLR is as under:

- ACM[1]
- IEEE[2]
- Scopus[3]
- Springer[4]
- Web of Science[5]

3.1.4. Defining the inclusion and exclusion criteria

The criteria for inclusion and exclusion of the searched items were defined to retain only the items that align with the goals of the study and help answer the research questions. The following inclusion criteria (IC) and exclusion criteria (EC) were defined and applied for this study.

- IC 1: The publication reports at least one mitigation strategy against phishing attacks.
- IC 2: The language of the publication is English.
- IC 3: In case the same strategy was reported in more than one publication, the most recent one was retained.
- IC 4: The publication has been published in a peer-reviewed journal or a conference.
- EC 1: Publications that have missing abstracts/meta-data.
- EC 2: Publications whose full-text version is not available.

[1] https://dl.acm.org.
[2] https://ieeexplore.ieee.org.
[3] https://www.scopus.com.
[4] https://link.springer.com.
[5] https://www.webofscience.com/wos/woscc/advanced-search.

It is relevant to mention that some mitigation strategies are reported in more than one publication, for instance, the first publication reports the initial version, and the subsequent one reports an improved version of the same. Therefore, IC 3 was formulated to include the most recent version of mitigation strategies reported in more than one publication. Moreover, concerning EC 1, it is important to mention that the meta-data for a publication includes: details of authorship, copyright year, date of publication; and other descriptive elements such as keywords and abstracts; or any identifying numbers (such as DOI). Therefore, the publications lacking these details were excluded.

3.2. Conducting the SLR

The search query mentioned above was used to search across selected databases and digital libraries listed earlier. The initial search revealed 4263 publications. Due to the large number of publications, we applied the publication time filter to include publications between 2018 and 2023. The literature search was conducted on the last day of March 2023; thus, only publications until that day were included for 2023. The application of the date filter reduced the number of publications to 2372. In the next step, the duplicate publications were removed, which reduced the total number of publications to 2024. During the initial screening phases, 1734 papers were screened after reading their title and abstracts. The screening was done based on the inclusion and exclusion criteria listed earlier. After the screening process, 324 publications were eligible for reading the full text. Furthermore, after reading the full text, 76 more publications were removed for not satisfying the inclusion criteria. Finally, 248 publications were included in this study. The number of papers across each database and digital library during different phases of this study is listed in Table 2.

Furthermore, to effectively execute and report this process, we incorporated elements of preferred reporting elements for systematic review and meta-analysis (PRISMA) methodology. The Fig. 1. summarizes the entire process of selection of publications using the PRISMA method.

For each eligible article, the following details were extracted from and added into a data repository (maintained in Microsoft Excel) for further analysis, these details include:

- Title of the publication
- Name of the proposed solution (if specified)
- Classification
- Description of the proposed solution
- Targeted phishing vector (email, eFax, Instant Messaging, SMS, Social Network, Vishing, etc.)
- The underlying technology for the solution (machine learning, cryptography, hardware-based, etc.)

The final dataset (see Appendix II) was analyzed to answer the research questions considered in this study; more details about the analysis and outcomes are presented in the following sections.

4. Reporting the results

This section presents the outcomes of the SLR framed along with the research questions presented earlier.

4.1. What mitigation strategies against phishing attacks have been proposed in the existing literature?

In our pursuit of finding an answer to this research question, firstly we looked up existing classification schemes for mitigation strategies against phishing attacks. This would have meant

Table 2
Number of papers across different digital libraries

Digital libraries	Initial search results	Results after applying the time filter	Results after removal of duplicates	Results after initial screening	Eligible publications for the study
ACM	330	134	106	36	32
Scopus	1721	1003	851	57	52
IEEE	523	307	295	86	70
Web of Science	680	372	229	91	75
Springer	1009	556	543	54	19
Total	**4263**	**2372**	**2024**	**324**	**248**

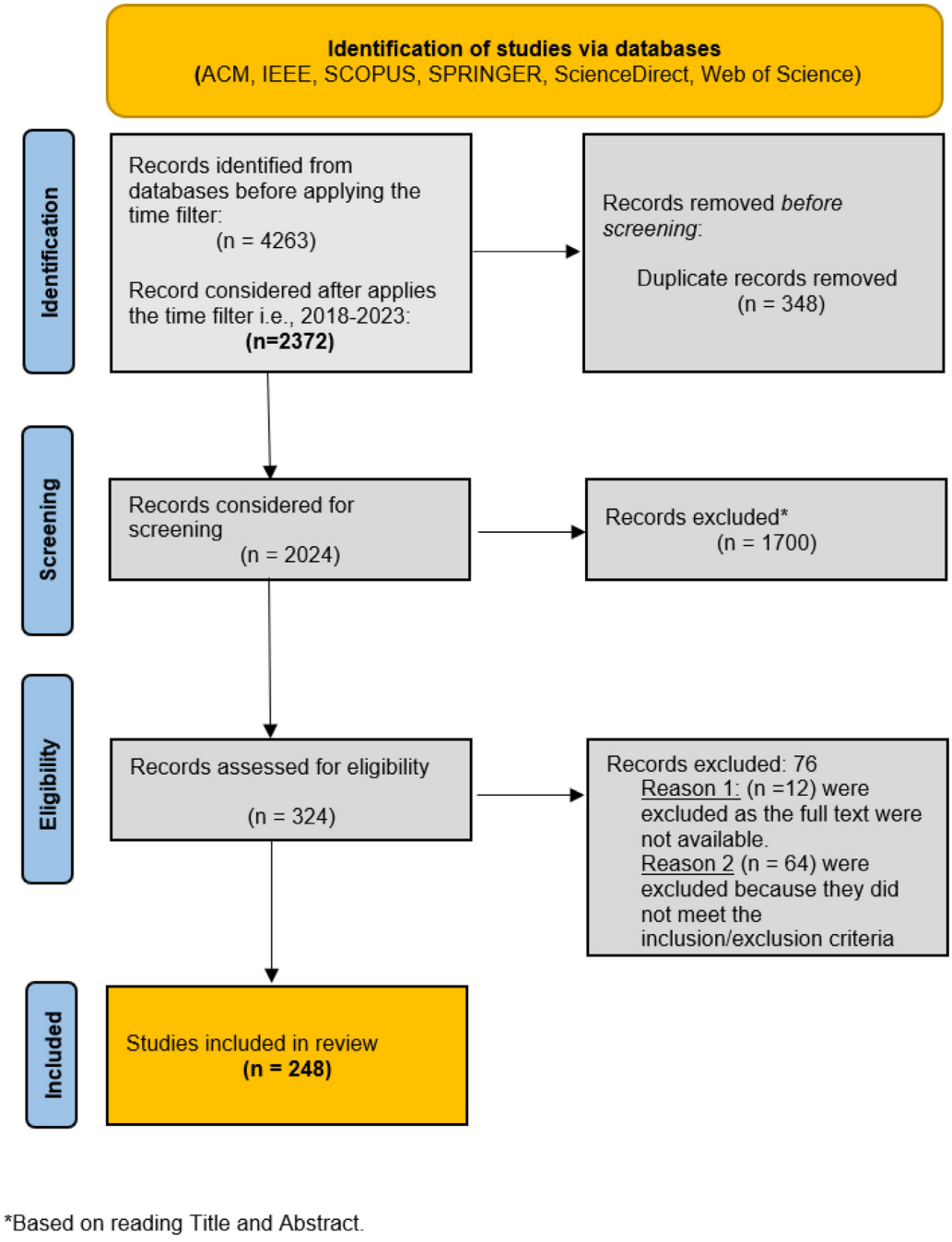

Fig. 1. PRISMA flow diagram summarizing the selection of publications

Fig. 2. Word cloud generated based on author keywords and index terms

mapping the dataset of this SLR according to those classification schemes. However, the classification schemes which exist (Chanti and Chithralekha, 2020; Apandi et al., 2020)) did not apply. The main reason for the lack of applicability is that these classification schemes were not designed for classifying a such broad range of data (as in this SLR) that considers mitigation strategies against phishing holistically by not limiting to any specific attack vectors.

Further, we analyzed the author keywords and index terms across all publishers to identify patterns for classifying anti-phishing strategies. To visualize the keywords in terms of frequency of occurrence a word cloud as presented in Fig. 2. was generated. It is evident from Fig. 2 that the terms such *as 'system', 'tools', and 'learning'*, which are relevant from a classification of mitigation strategies perspective appear, however, these are not complete for the classification of mitigation strategies considered in this SLR.

Finally, a three-step *coding and labeling* approach was used to identify the categories for classifying the mitigation strategies against phishing attacks. The first step was the assignment of codes to publications for identifying 1st order concepts. Based on the similarities between several 1st-order concepts, more abstract 2nd-order concepts were identified. Finally, the 2nd order concepts were grouped to form aggregate concepts for classifying the mitigation strategies against phishing attacks. The process just discussed is presented in Fig. 3. It is important to add an interpretation of these terms as developed after analysis of the existing literature.

- **Anti-phishing systems:** this category refers to software and tool-based strategies for mitigating phishing attacks. These include stand-alone systems, program design approaches, and tools for mitigation purposes.
- **Models and frameworks:** this category refer to models and frameworks that aid in mitigation against phishing attacks. The category includes (1) frameworks that govern a series of activities to mitigate phishing attacks, and (2) models and methods including machine learning-based models to enhance the anti-phishing capabilities of newer and existing systems.
- **Human-centric mitigation strategies:** this category refers to influencing the capacity and capability of human users in better detecting and mitigating phishing attacks. This category mainly includes guidelines & recommendations to improve such abilities, for example, planning and executing anti-phishing training, conducting evaluation quizzes, etc.

As mentioned in Fig. 3, the full texts of all publications (n=248) considered in this SLR were analyzed to assign 1st order codes for identifying the concept for each publication. The 1st order concepts were merged to form abstract 2nd order concepts, which were ultimately merged to identify aggregate concepts for classifying the publications. All publications classified in line with the scheme just discussed are presented in Appendix II.

It is relevant to state that most publications are classified as anti-phishing systems (see Fig. 4) as they present standalone anti-phishing systems, tools to mitigate phishing, or design approaches and algorithms for developing anti-phishing strategies. For instance, Valentim et al. (2021) present a Generative Adversarial Network (GAN) based approach to automate the generation of new squatting candidates from a list of benign URLs. The results show that the approach successfully generated new squatting candidates that were previously unknown. Similarly, Drichel et al., (2021) proposed an anti-phishing system based on detecting phishing attacks already during the website preparation by monitoring the certificate transparency logs. The authors presented a pipeline that facilitates such evaluations. The system was tested on several new and existing classifiers with great accuracy.

As presented in Fig. 4, several models and frameworks have also been proposed. For instance, Ozcan et al. (2021) presented a hybrid deep learning approach based on long short-term memory (LSTM) and deep neural network algorithms (DNN) for detecting phishing URLs. The results showed that their hybrid approach achieved better performance in terms of detecting phishing URLs. Lastly, less in number than the other two of the categories, human-centric mitigation strategies have been proposed. These mainly include the guidelines and recommendations for improving end-users' abilities to detect and mitigate phishing attacks (for instance, (Sadiq et al., 2021)). However, some training and awareness schemes have also been proposed (for instance, (Wash, 2020).

We further analyzed the dataset to identify the concepts and technologies considered in the development of mitigation strategies. It was identified that the mitigation strategies mainly use the following concepts and technologies:

i Machine learning
ii Neural Networks
iii Deep Learning

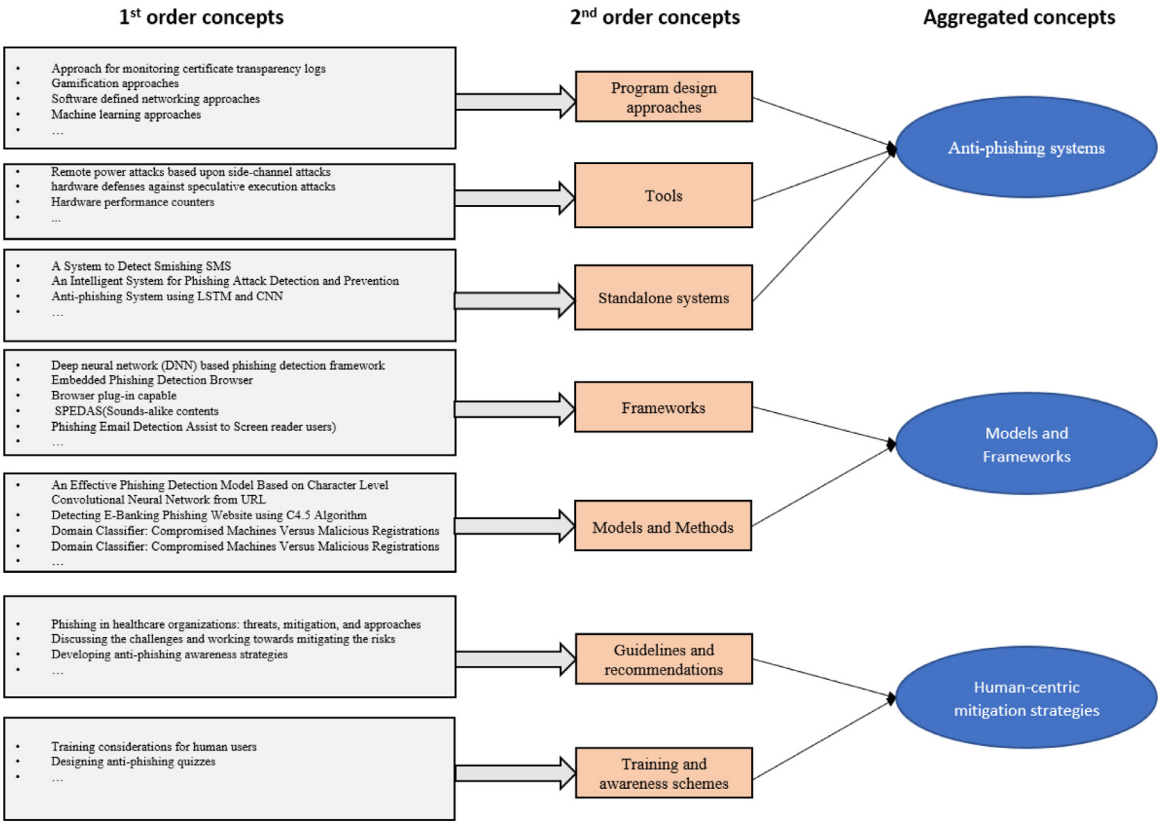

Fig. 3. Classification schemes for mitigation strategies against phishing attacks

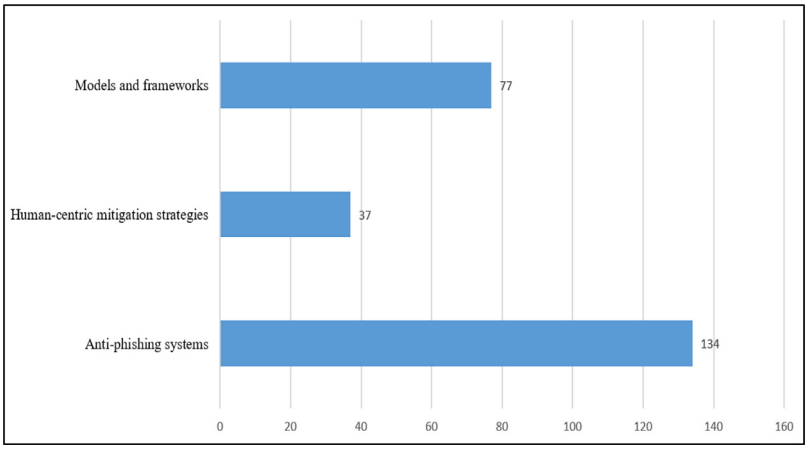

Fig. 4. Classification of existing mitigation strategies against phishing attacks (n=248)

iv Cryptography
v Human-centric mitigation strategies

Each of these categories refers to a set of techniques that have been proposed to mitigate phishing attacks. For instance, different machine learning approaches, such as graph inference, vector machines, and logistic regression, among others, have been proposed under the machine learning category. More details concerning these categories and the specific algorithms and techniques are presented in Fig. 5. It is important to note that in addition to the concepts and technologies mentioned above, one category 'Others' was created to group technologies with a relatively lesser number of mitigation strategies appearing in the dataset of this SLR. This category includes, for instance, mitigation strategies based on natural language processing, software-defined networks, gamification, and blockchain, among others.

Furthermore, we analyzed the number of solutions related to similar underlying concepts and technologies (as presented in Fig. 5). It was, therefore, revealed that using different machine learning-based algorithms and techniques has been the most prevalent approach while proposing mitigation strategies. More details about the number of publications related to specific concepts and technologies are presented in Fig. 6.

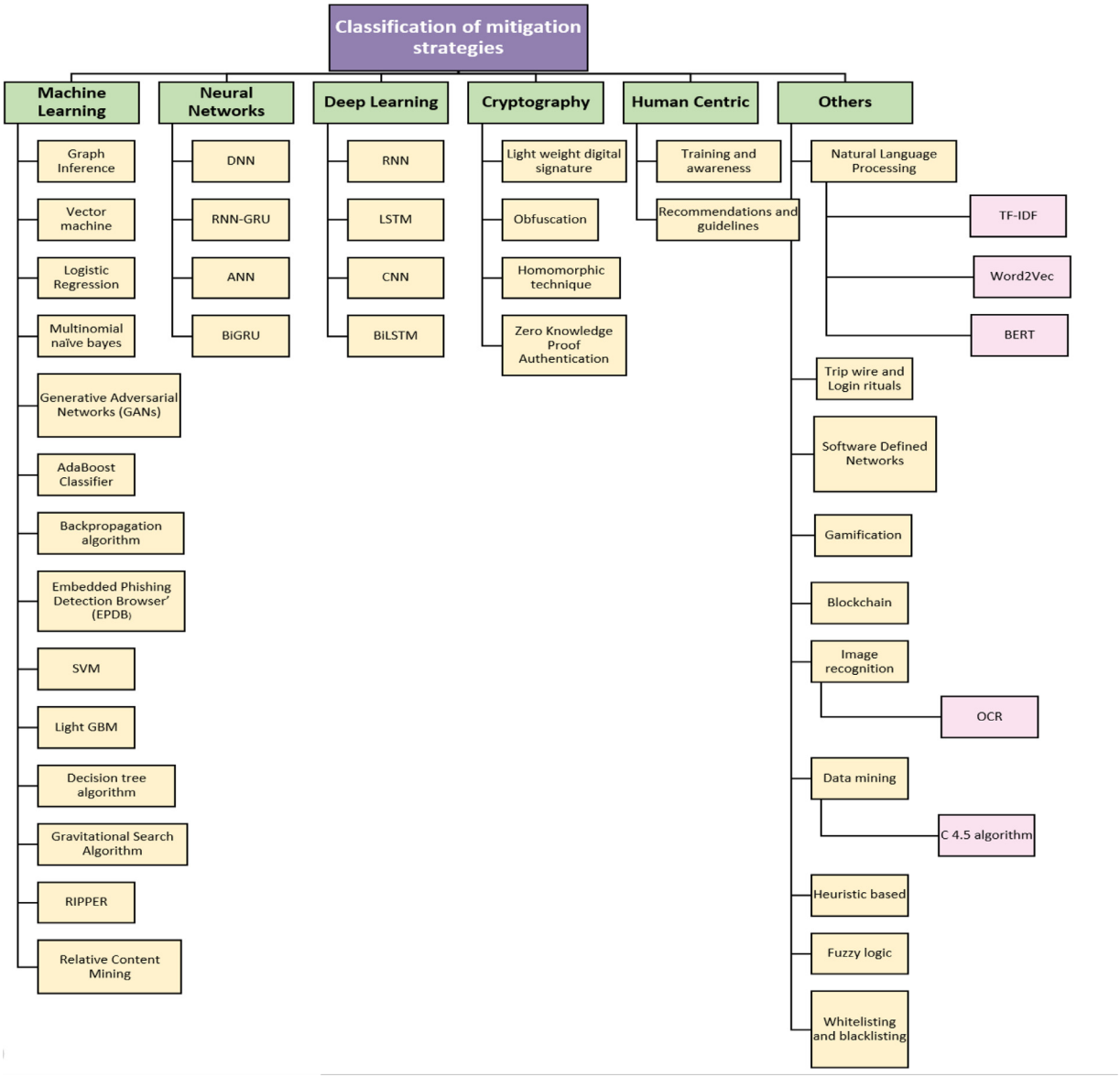

Fig. 5. Classification of mitigation strategies against phishing attacks based on the underlying technology

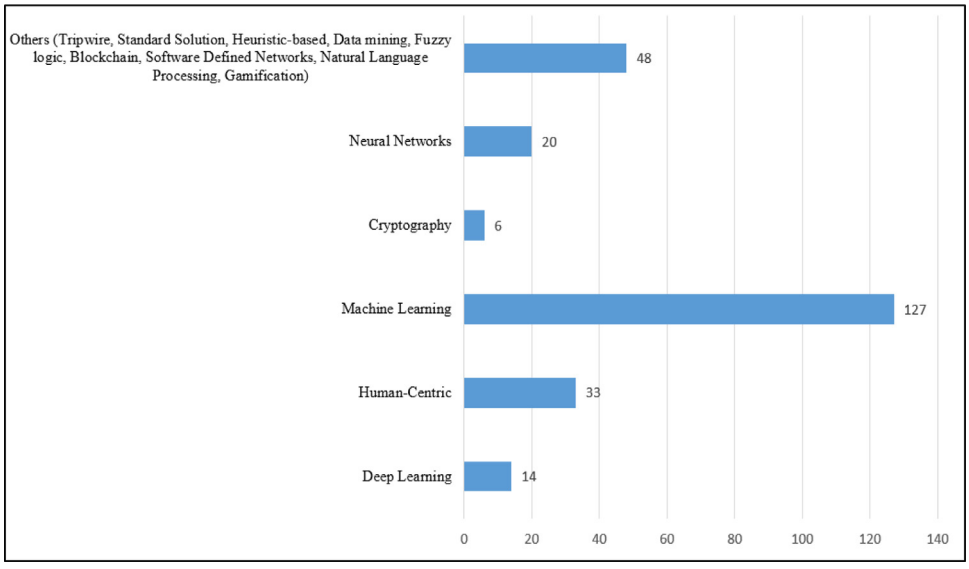

Fig. 6. Underlying concepts/technologies considered in the mitigation strategies (n=248)

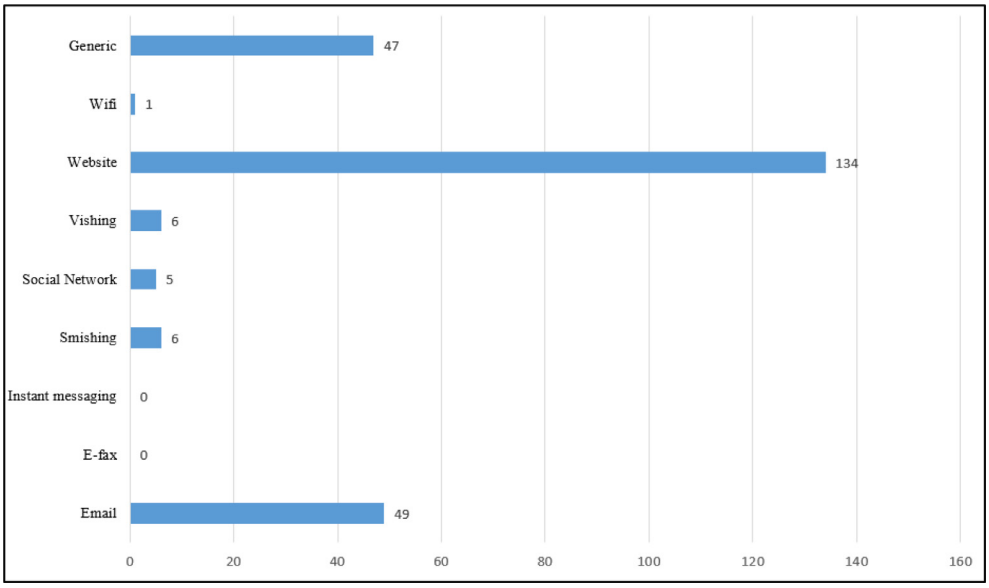

Fig. 7. Focused attacks vectors in the mitigation strategies (n=248)

4.2. Which phishing vectors have been mostly considered in the development of mitigation strategies?

Before discussing the outcomes of this SLR in line with the second research question, it is important to mention that the phishing vectors considered during this study have been identified from the framework presented by Chiew et al. (2018). Chiew et al. (2018) report that three mediums, (1) the Internet, (2) short messaging service, and (3) voice, can be used for executing a phishing attack. Within each of these mediums, different phishing vectors can be used. For instance, for the Internet as a medium, phishing vectors including (a) email, (b) eFax, (c) instant messaging, (d) social media networks, (e) websites, and (f) Wi-Fi are often used, similarly, for short messaging service as a medium, vector such as *smishing* are used, however, in the case of voice as a medium, *vishing* is often used as an attack vector. Furthermore, for any of these vectors, the attacker can employ different technical approaches to execute the phishing attack. For example, attack vectors to target a website may include, exploiting browser vulnerabilities, clickjacking, cross-site scripting, and man-in-the-middle attack. However, further details concerning the inter-relation between medium, vectors, and technical approaches to phishing are presented in the existing work (Chiew et al., 2018).

The publications considered during this SLR were analyzed to identify the phishing vectors targeted in the proposed mitigation strategies. The targeted phishing vectors were mentioned explicitly in most of the records, however, in case it was not mentioned, the authors analyzed the mitigation strategy to check if it aligns with mitigating against a particular phishing vector, if not, it was labeled under the 'generic' category. The details of phishing vectors most considered in the development of the mitigation strategies are presented in Fig. 7.

It is evident from the bar plot in Fig. 4. that the most focused phishing vector during the development of mitigation strategies is phishing through websites. A total of 134 publications report a mitigation strategy against phishing through websites, these also include phishing attempts using QR codes. Furthermore, 49 publications reported mitigation strategies against email-based phishing attacks. There were 47 generic anti-phishing strategies, which did not target any phishing-specific vectors or worked well for multiple phishing vectors. These mainly include frameworks to protect against phishing attacks (Younis and Musbah 2020), and phishing awareness strategies (Dukarm, Dill, and Reith, 2019). There were 6 publications each focusing on mitigating phishing initiated through smishing and vishing, however, 5 publications focused on phishing attacks using social networks as an attack vector. Finally, 1 publication focused on mitigating phishing initiated by using Wi-Fi as a vector. However, as shown in Fig. 4., no mitigation strategies were proposed for e-Fax and instant messaging.

4.3. What anti-phishing guidelines and recommendations (for organizations and end-users) can be synthesized from the existing literature?

Having reviewed the existing literature on the topic and categorizing it, we synthesized the guidelines and recommendations from existing literature that could aid in mitigating phishing attacks. These recommendations and guidelines are grouped based on their relevance for (1) organizations and (2) end-users.

4.3.1. Anti-phishing guidelines and recommendations for organizations

In total, 54 anti-phishing guidelines and recommendations for organizations were extracted from the existing literature. A synthesis of the detailed guidelines and recommendations extracted from the existing literature is presented in Table 3.

As shown in Table 3. the extracted guidelines and recommendations are grouped into 6 categories:

- Follow security policies.
- Implement access control.
- Implement endpoint security.
- Use training and awareness programs.
- Implement policies for devices.
- Keep in mind the advice.

The detailed description of each of the categories with reference to the existing literature is as follows.

- **Training sessions and awareness programs:** Cybersecurity training is the perfect way to raise awareness about common phishing tactics. An organization must have a training program

Table 3
Anti-phishing guidelines and recommendations for organizations

Recommendations for organizations	Main categories of guidelines	Guidelines
	Follow security policies	- Adapt company policy to include specific security and anti-phishing training opportunities, especially for risky users and high-risk users. - Implement reporting protocol. - Create secure routines. - Respect and engage employees. - Protect productivity. - Set up and enforce password protection policies. - Exchange potential threats, indicators of compromise, and best practices in house - Implement Backup Strategies - Create privacy-conscious data sharing and processing. - Implement a Standard Solution (SS) where several sets of guidance can be written by a qualified person and then re-used.
	Implement access control	- Implement web tripwires. - Implement administrative multifactorial authentication like MFA Microsoft Multi-Factor Authentication. - Use DMARC email authentication. - Use login rituals.
	Implement endpoint security	- Develop an intelligent networking threat detection system. - Update Computer hardware and software periodically. - Use firewalls, updated antivirus programs, email blockers, and browser extensions. - Use host-based intrusion detection systems (HIDS). - Follow vendor's security manuals.
	Use training and awareness programs	- Use embedded training for better education. The training material must be displayed as soon as a mistake is made. - Develop on-site and personal device physical security awareness. - Use deception cues-based training. It can be effective in diverse deceptive contexts. - Use a human-centered design (HCD) approach for the development of cyber training. - Conduct on-site anti-phishing training, use quizzes for evaluation, and virtual labs for education. - Use web platforms for improving cognitive processes in people during the process of detecting phishing attacks. - Use virtual learning tools, simulations for training, and gamification approaches. - Use self-explanatory training material that provides information on why the user is being presented with that. - Use CRI to determine how much and what type of training employees need. - Never ask employees for secure behavior unless you have checked if it is possible to do in their work environment. - Actively phish users and, when they get caught responding to phishing emails, present them with short, easy-to-read training material on how to recognize phishing attempts in the future.
	Implement policies for devices	- Develop and budget for life-cycle management to retire devices that cannot be replaced right away. - To maintain a regularly updated inventory of all devices on the network (authorized and unauthorized). - Create a policy that enables timely updates through collaboration with the external manufacturing community and internal stakeholders. - Develop a patching policy that minimizes equipment downtime. - Evaluate the expected lifetime of devices before purchase.

	Keep in mind the advice	- Verify all incoming calls for the authority.
		- Do not share any information until and unless the contact made by the other person was expected.
		- Hire cybersecurity professionals.
		- **For Board members**
		  ◦ Build secure routines.
		  ◦ Develop meaningful metrics (such as training completion rates or percentages of staff clicking on phishing emails).
		  ◦ Practice secure behaviors.
		  ◦ Buy a standard security awareness package.
		- **For CISOs**
		  ◦ Find low-friction solutions.
		  ◦ Focus on routines employees should follow to do their job securely.
		  ◦ Changing behaviors in cybersecurity requires long-term planning and resources.
		  ◦ Remember that staff need to feel secure, connected, and believe in their future.
		- **For executives**
		  ◦ Create low-friction solutions and integrate security into business processes.
		  ◦ Encourage staff to participate in security.
		  ◦ Lead by example.
		  ◦ Bring together different skills and capabilities.
		- **For security professionals**
		  ◦ Be approachable and helpful.
		  ◦ Use respectful language.
		- **For security awareness specialists**
		  ◦ Do constant evaluation (what works, and what does not).
		  ◦ Identify which groups need what awareness and training, and how best to deliver it.

about phishing (Jampen et al., 2020). Awareness sessions and teaching programs can also be offered through seminars, conferences, and other virtual learning tools. Information programs may include conferences, information campaigns, and thematic training. Similarly, teaching methods can utilize virtual laboratories, simulators, games, and modern applications (Mashtalyar et al., 2021). Effective and well-founded anti-phishing training programs must begin with "dedication" because training sessions in the form of courses have the greatest effect on short-term learning. After this initial step, program participants must complete training using the built-in training. For example, a CRI method can be used to determine the number and types of training employees need (Jampen et al., 2020). Besides, only the provision of training materials does not contribute to the detection of phishing and may even undermine the trust of users. Existing efforts to train users to protect against phishing emails are mainly focused on a small number of domains that may prove ineffective in other areas. To eliminate this limitation, learning based on deception signals can be effective in various deception contexts, since this learning method uses the linguistic features of the email itself (Lim et al. 2021). It would be useful to help people connect the common characteristics of phishing emails (such as action links) to phishing in general. It is because these features enhance people's memory of phishing as an alternative explanation (Wash, 2020).

One approach proposed by Lim et al., (2021) is to actively send phishing emails to users and, when they are caught responding to an email from a phishing attack, provide short and simple training materials demonstrating how to recognize an attack. Training material should be displayed immediately after mistakenly clicking on a link in an e-mail. On the other hand, the presentation of training materials may be delayed until certain additional steps have been taken, e.g., after the credentials have been entered on a fake organization login page (Jampen et al., 2020). Nevertheless, these occurrences are complicated because if a user clicks, but does not enter his credentials, training may still be required to recognize phishing attempts based on email content and links. Furthermore, if the employee does not click the link in a phishing email, but does not report the phishing attempt either, there needs to be a customized training package explaining why it is important to report the phishing attempts (Jampen et al., 2020). This is also relevant from the perspective of using machine learning-based approaches, as such reporting helps in training the system for accurate detection.

- **Implement endpoint security:** Endpoint security includes updated antivirus, malware, and host-based intrusion detection systems (HIDS). Another option for prevention is using a new generation of malicious email blockers that each email service provider can use to prevent malicious emails from reaching customers (Mashtalyar et al., 2021). A strong firewall and infrastructure can mitigate some cyber-attack risks by restricting access to company systems, even if the device is compromised. For instance, intelligent networking threat detection systems, and DMARC email authentication (Priestman et al., 2019). In addition, the use of the following, implementing backup strategies, installing, and updating protective software, blocking pop-ups, and updating the computer hardware is also advised. (Manjezi and Botha, 2018).
- **Implement access control:** Organizations must establish and implement appropriate password protection policies and information exchange policies (Argaw et al., 2019). It is also advised to use the web tripwire and the login rituals – which are based on deception to extend the authentication of the web application. Tripwires and rituals do not suffer from the reuse problem that is typical for passwords. They can be integrated with existing Microsoft Multi-Factor Authentication (MFA) systems to increase account security in cases of complex phishing attacks. In addition, the use of MFA will significantly reverse the flow of Office 365 accounts that have been compromised (Moul, 2019).
- **Implement security policies:** Cybersecurity measures should be based on vulnerability management, potential threats, compromise indicators, and practices in the exchange, sharing, and processing of privacy-conscious data (Argaw et al., 2020). The same needs to be reflected in the security policies (Manjezi and Botha, 2018). Security policies need to be implemented continuously by reaffirming basic security practices, such as password policies, and the implementation of reporting protocols, paying more attention to staff training and education, and raising awareness about physical security on-site and personal devices (Priestman et al., 2019).

To transfer authority between multiple teams to find solutions and implement them, a Standard Solution (SS) can be implemented in the manual in which a qualified specialist can write several sets of instructions and then reuse them. The availability of servers is also useful for supporting employees who are not phishing experts themselves. This solution can also quickly provide consistent professional recommendations and detailed steps. SS towards mitigating the phishing attacks aims at, for instance, expressing gratitude to users who successfully identify and report phishing emails and can distinguish between phishing and legit emails; furthermore, SS can assist users who reportedly click the links in the phishing emails. (Althobaiti, Jenkins, and Vaniea, 2021).

- **Implement policies for devices:** There should be policies for devices as well duly catering to different phases of their operation. The decision-makers assess the expected life expectancy of devices (e.g., support from manufacturers/suppliers or support from operating systems). There needs to be a repair policy to minimize equipment outage time and to ensure timely updates in cooperation with external manufacturing teams. Organizations should also develop and allocate life cycle management funds to dismantle equipment that cannot be replaced immediately. There must be a regularly updated registry of every device being used in the organization (Argaw et al., 2020).
- **Keep in mind the advice:** In any organization, the employees should not share any information with unknown people by any communication means. The employees also need to avoid reciprocity as attackers attack only those who reciprocate the initial attempts at contact. The attackers can also use correct information about the health status of an employee or any member of their family to sound relevant. This can also include any other information that attackers can get their hands on (Venkatesha, Reddy, and Chandavarkar, 2021). Therefore, the employees must ascertain the need behind a certain action before executing it. Finally, organizations must hire cybersecurity professionals (Manjezi and Botha, 2018). Finally, advice for specific roles in the industry including board members, CISOs, and security professionals has been presented.

4.3.2. Anti-phishing guidelines and recommendations for end-users

In total, 23 anti-phishing guidelines and recommendations were extracted for the end-users. A synthesis of the detailed guidelines and recommendations extracted from the existing literature is presented in Table 4.

As shown in Table 4, the guidelines and recommendations for end-users are classified into the following two categories:

- Use awareness as the mitigation strategy.
- Use security advice.

Table 4
Anti-phishing guidelines and recommendations for end-users

	Main categories of guidelines	Guidelines
Recommendations for end-users	Use awareness as the mitigation strategy	- Be extra careful with emails from unknown or dubious origins. - Do not trust emails from anon senders. - When in doubt contact a professional in the area for help. - Delete the phishing email without opening it. - Never share your personal information unless sure about the origin. - Think twice before you click. - Be wary of pop-ups.
	Use security advice	- Update computer hardware and software. - Use antivirus software. - Check your online account regularly. - Use strong passwords, do not pretext them. - Verify a site's security. - Look up web pages, and security certificates. - Should not use the same password for multiple accounts. - Ensure that the website URL starts with https:// - Avoid using public computers for handling confidential information. - Do not leave your computer unattended. - Do not open attachments in emails by unknown senders. - Do not click on the links in emails by unknown senders. - Use 2FA via an authentication app. It is the preferred choice over SMS /voice authentication. - When unsure, use tools to check suspicious links before opening. - Block Pop-Ups. - Use the browser's phishing list.

Each of these categories is discussed below.

- **Use awareness as the mitigation strategy:** The following methods against phishing attacks should be used by the end-users, use the browser's anti-phishing function, use sites to test links, and use your skills to prevent cyber-attacks (Venkatesha, Reddy, and Chandavarkar, 2021). Other suggestions include thinking before clicking, installing a phishing anti-attack toolbar, keeping the browser up to date, using firewalls, checking site security, being careful of the pop-ups, do not share personal information, use antivirus software (Sadiq et al., 2021). Argaw et al. (2019) identify that end-users should not use the same password on multiple accounts, should not keep the computers unsupervised, and must not trust emails from unknown senders.
- **Use security advice:** Users should be more attentive to their computer security. For example, they should avoid using public computers when handling confidential information. The users must also maintain antivirus software and update programs regularly. They need to take special care with emails of questionable origin. Strong authentication can protect users from many identity attacks, thus reducing the probability of security breaches. To ensure the best protection and user experience, it is recommended to use authentication options without a password (Venkatesha, Reddy, and Chandavarkar, 2021). End users should check whether the web pages they visit are completely reliable and whether they have a valid security certificate or not. Moreover, the website address usually should start with 'https://'. If a user has doubts, they should seek advice from a specialist in the field (Jampen et al., 2020).

It is important to note that the guidelines and recommendations mentioned in this Section reflect what was extracted from the source publications considered in this SLR. However, in addition to these guidelines, other relevant guidelines from sources such as gray literature (for instance, Ellis, 2023; Milnsbridge, 2023) might be useful specifically for the end users. For instance, for the user to make accurate decisions on classifying an email as phishing, they must know the characteristics of a phishing email, which generally include, the phishing email has suspicious words, phrases, or sentences, it has suspicious links, it has grammatical or spellings errors in the body, it starts with a generic greeting, it contains pop-up boxes or attachments, it contains an air of urgency or a need to respond immediately, and it asks for personal information or details such passwords, social security number.

The guidelines and recommendations presented in Tables 3 and 4 have been synthesized from academic literature. It is relevant to note that the literature was analyzed qualitatively to extract these guidelines and recommendations. Furthermore, an interesting aspect from the perspective of future work is to quantify these guidelines and recommendations in terms of their effectiveness both for the organizations and end-users respectively. This could either take the form of a longitudinal study to assess the effectiveness of these guidelines and recommendations or a focus group comprising of industry experts could be held to quantify the impact of these guidelines and recommendations. The threats to the validity of the quantification approach must be addressed in the study design.

4.4. What gaps and open issues emerge from the analysis of the existing literature?

Phishing continues to pose a serious threat to people and organizations. While several mitigation strategies (as discussed earlier) have been developed to mitigate phishing attacks, there are still certain outstanding concerns and gaps in their effectiveness. One such gap that was identified during the analysis of the SLR dataset is that most of the anti-phishing mitigation strategies are technology-centric i.e., the use of different technologies has been proposed in the development of those strategies. However, what appears to be missing is the focus on the role of humans using these technologies. To overcome this gap, what needs to be considered in conjunction with the development of technologies is to equip the users with elements of security literacy, thereby assisting in making accurate security decisions when confronted with a challenge.

Furthermore, one other concern revealed after the analysis of the state of the art is that there are several phishing vectors, such as vishing, smishing, instant messaging, and Wi-Fi, for which many

mitigation strategies have not been proposed. Therefore, in such cases, the gaps and concerns are more about the completeness and catching up required in the state of the art than the efficacy of each mitigation strategy. Following are the gaps and open research questions which emerge after the analysis of the SLR.

4.4.1. Human-centric gaps and open issues

Following are the human-centric gaps and open issues that pose challenges in the pursuit of mitigating phishing attacks:

- **Risk-taking behavior is an issue for phishing prevention:** Humans are often considered the weakest link in the security chain. The overall human risk in maintaining security hygiene is on the rise. Three aspects associated with these increased risk levels include, (1) more and more services are going digital, which means that people can use multiple devices from anywhere to get their job done which means that the number of endpoints and connections needing protection has increased; (2) it is in the human psychology that sometimes humans can be careless, take risks and fall for urgency, fear or emotions, which is one big challenge from a phishing perspective; and (3) lack of policies to address the human element in cyber security strategies (Babati, 2020). As stated earlier that humans can take risks and fall for urgency and other emotions, it is relevant to note that from a phishing perspective, such risk-taking behavior grows the likelihood of opening a phishing e-mail or clicking a link to a website. Analysis of existing work during this SLR identified that personal emotions such as fear, attraction, innocence, greed, or kindness might be exploited to expose sensitive information from the users (Dam & Deshpande, 2021). The open research questions in this regard include:
  - i How to limit the avenues of risky behavior by the end users?
  - ii What considerations need to be made towards the development of an anti-phishing strategy that also considers the personal emotions and risk-taking attitudes of the users?
- **Educating the users towards pro-security behaviour:** Despite ongoing education and awareness campaigns to raise awareness against phishing attacks, phishing trends continue to increase. There have been instances where people who trained for the identification of phishing attacks fell victim to phishing. This is because the attackers continually modify their attack strategies and use advanced social engineering techniques to deceive the users. One critical aspect to note here is that while education and awareness campaigns are important, it is even more critical to note that user behavior plays a key role in influencing the efficacy of phishing mitigation strategies. Educated and aware users might still fall victim to phishing if they are distracted or are using devices with small screens. The open research questions in this regard include:
  - i How to develop education and training content to influence users' behaviors?
  - ii How to design anti-phishing awareness campaigns while considering a diverse group of users with varying literacy levels?

4.4.2. Technology-centric gaps and open issues

Various technical solutions, as presented in Section 4 (see Fig. 5) have been proposed to detect and block phishing attempts, however, considering the phishing trends, it is evident that these solutions have not been effective in limiting successful attacks. Following are the technology-centric gaps and open issues that pose challenges in the pursuit of mitigating phishing attacks:

- **Development of foolproof mitigation strategies:** One obvious gap evident from the phishing trends is the current mitigation strategies have not been good enough to curb the phishing attempt. This is because the attacks have developed ways to bypass the protection mechanisms in place. For instance, multifactor authentication can be helpful against phishing attacks especially when the attacker aims to steal the credentials, however, multifactor authentication is no longer foolproof, as there have been instances of it being compromised. Furthermore, another aspect to consider in developing foolproof mitigation strategies is to consider their performance issues in terms of false positives and negatives. A false positive in the context of a spam filter would mean a legitimate email being flagged as phishing, which would cause confusion and frustration for the users. However, allowing a phishing email to pass to the user as a legitimate one is also crucial to consider.
  - i How to achieve a balance between false positives and false negatives associated with various anti-phishing mitigation strategies?
- **On the need for other methods to prevent phishing:** With reference to the discussion in Section 4.1, the use of different machine learning methods as the underlying technology appeared as the most prevalent way to mitigate phishing attacks. However, the phishing trends referred to at the beginning of this article point toward a continuous increase. The question is, do we need other approaches besides machine learning-based methods to prevent phishing attacks? Moreover, machine learning-based approaches have limitations in accuracy and performance, particularly in the case of 'zero day' phishing attacks (Alauthman et al., 2019). The open research questions in this regard are:
  - i How to overcome the limitations of machine learning-based strategies to identify zero-day phishing attacks?
  - ii What factors limit the accuracy and performance of machine learning-based strategies in specific contexts of use?
- **Consideration of phishing vectors in developing mitigation strategies:** As discussed in Section 4.2, most anti-phishing strategies are focused on websites and email-based phishing attacks. However, a relatively small number of anti-phishing strategies were reported for Wi-Fi, smishing, and social networks, and none for eFax and instant messaging vectors. It is critical to consider vectors other than email and websites in developing mitigation strategies. Furthermore, one issue that needs to be discussed here is the existence of generic strategies. It is relevant to mention that phishing is a highly context-specific attack, and developing generic strategies might not end as an optimal approach. The open research questions in this regard include:
  - i How to mitigate phishing attacks executed using vectors such as social media, instant messaging, and hosting fake Wi-Fi hotspots?

Finally, technology-centric solutions will never be enough unless human users are aware of the security practices and procedures, whether on user-owned devices or as part of the organization. Therefore, in developing the systems and services, the developers and designers must consider the security literacy of the intended users while delegating security decisions to them. Furthermore, it is also important to develop specific training programs and awareness campaigns to educate the users on the elements of security literacy and thus enable them to prevent, detect and report phishing and other cyber security attacks.

5. Conclusion

The paper presents the outcomes of SLR conducted while focusing on four research questions. The paper advocates that technology-only solutions are never going to be enough to protect

against attacks targeted toward human users, therefore, there is a need to consider the role and abilities of human users in the development of anti-phishing mitigation strategies.

In line with the research questions, the paper identifies and classifies existing mitigation strategies against the phishing attacks. Most of the mitigation strategies are based on machine learning algorithms as the underlying technology. Furthermore, a majority of the mitigation strategies considered in this SLR were developed considering websites and emails as attack vectors for phishing attacks. Open research questions and gaps in the state of the art are also discussed in the paper. In addition, the paper also presents 77 guidelines and recommendations for organizations and end-users to assist in mitigating against the phishing attacks.

It is important to note that the paper only considers publications over the last five years (at the time of writing), starting in 2018 until March 2023. This means that some significant mitigation strategies not falling under this timeline might have missed out on the state-of-the-art presented in the paper. Furthermore, there could be other relevant papers on the topic discussed in this paper, however, such papers could not be included for not fulfilling the inclusion criteria or for being published after the submission of this work.

Finally, the paper targets researchers, industry practitioners, and a general audience interested in cyber security. For researchers, it provides a classification of the existing solutions along with open issues and research questions to help drive future research. For industry practitioners, it presents a review of state-of-the-art concerning phishing attacks, the guidelines, and recommendations specifically from the organizations' perspective that might be useful for implementations in their organizations. For the general audience interested in cyber security, the paper highlights the current trends concerning phishing and summarizes the state of the art of mitigation strategies.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Bilal Naqvi reports financial support was provided by Business Finland.

Data availability

Data will be made available on request.

Appendix-I

Reformatted search queries across different databases

* **ACM**

- [Title: phishing] AND [[Title: guidelines] OR [Title: best practices] OR [Title: tools] OR [Title: prevention techniques] OR [Title: prevention] OR [Title: mitigation] OR [Title: solutions]] AND [E-Publication Date: (01/01/2018 TO 12/31/2023)]
- [Abstract: phishing] AND [[Abstract: guidelines] OR [Abstract: best practices] OR [Abstract: tools] OR [Abstract: prevention techniques] OR [Abstract: prevention] OR [Abstract: mitigation] OR [Abstract: solutions]] AND [E-Publication Date: (01/01/2018 TO 12/31/2023)]
- [Keywords: phishing] AND [[Keywords: guidelines] OR [Keywords: best practices] OR [Keywords: tools] OR [Keywords: prevention techniques] OR [Keywords: prevention] OR [Keywords: mitigation] OR [Keywords: solutions]] AND [E-Publication Date: (01/01/2018 TO 12/31/2023)]

IEEE

- "Phishing" AND ("guidelines" OR "best practices" OR "tools" OR "prevention techniques" OR "prevention" OR "mitigation" OR "solutions")

Web of Science:

- ALL= (“Phishing” AND (“guidelines" OR "best practices" OR "tools" OR "prevention techniques" OR "prevention" OR "mitigation" OR "solution"))

***SCOPUS:**

- TITLE-ABS-KEY (“Phishing” AND ("guidelines" OR "best practices" OR "tools" OR "prevention techniques" OR "prevention" OR "mitigation" OR "solution")) AND (LIMIT-TO (PUBYEAR, 2023) OR LIMIT-TO (PUBYEAR, 2022) OR LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018))

Springer:

- '"Phishing" AND ("guidelines" OR "best practices" OR "tools" OR "prevention techniques" OR "prevention" OR "mitigation" OR "solutions")'

*Title-Abstract-Keyword search was performed to limit irrelevant publications appearing in the search

Appendix-II

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
1	Finding Phish in a Haystack: A Pipeline for Phishing Classification on Certificate Transparency Logs	Anti-phishing systems	Website	Machine Learning (Random Forest, DL (RNN, LSTM))
2	A Framework to Protect Against Phishing Attacks	Human-centric mitigation strategies	Generic	Gamification
3	A Phishing Mitigation Solution Using Human Behaviour and Emotions That Influence the Success of Phishing Attacks	Human-centric mitigation strategies	Website	Machine Learning (Risk score calculator)
4	Following Passive DNS Traces to Detect Stealthy Malicious Domains Via Graph Inference	Anti-phishing systems	Website	Machine Learning (Graph Inference)
5	Human Risk Factors in Cybersecurity	Human-centric mitigation strategies	E-mail	Easy-to-read documents
6	A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection	Anti-phishing systems	E-mail	Natural Language Processing and Machine Learning (TF-IDF, Word2Vec, and BERT NLP)
7	Click This, Not That: Extending Web Authentication with Deception	Anti-phishing systems	Website	Tripwire and login rituals
8	PhAttApp: A Phishing Attack Detection Application	Anti-phishing systems	E-mail	Machine Learning
9	Secure Email Login Based on Lightweight Asymmetric Identities	Anti-phishing systems	E-mail	Cryptography (Light weight digital signature)
10	A Flexible Phishing Detection Approach Based on Software-Defined Networking Using Ensemble Learning Method	Anti-phishing systems	Website	Software Defined Networks
11	Detecting Telephone-Based Social Engineering Attacks Using Scam Signatures	Anti-phishing systems	Vishing	Machine Learning
12	How Experts Detect Phishing Scam Emails	Human-centric mitigation strategies	E-mail	Training and awareness
13	Detecting Spam Tweets Using Machine Learning and Effective Preprocessing	Anti-phishing systems	Social Network	Machine Learning (Vector Machine, Logistic Regression, Multinomial Naive Bayes, and Neural Network)
14	Augmenting Phishing Squatting Detection with GANs	Anti-phishing systems	Website	Machine Learning (Generative Adversarial Networks (GANs))
15	Visualizing and Interpreting RNN Models in URL-Based Phishing Detection	Models and Frameworks	Website	Deep learning (RNN)
16	Avoid Phishing Traps	Human-centric mitigation strategies	Generic	Training and awareness
17	A Design of an Anti-Phishing Training System Collaborated with Multiple Organizations	Human-centric mitigation strategies	Generic	Training and awareness
18	LinkMan: Hyperlink-Driven Misbehavior Detection in Online Security Forums	Anti-phishing systems	Website	Machine Learning
19	URL-Based Phishing Detection Using the Entropy of Non-Alphanumeric Characters	Models and Frameworks	Website	Randomization
20	What.Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game	Human-centric mitigation strategies	E-mail	Gamification
21	PhishLedger: A Decentralized Phishing Data Sharing Mechanism	Anti-phishing systems	Website	Blockchain (Hyperledger Fabric)
22	Machine Learning for Tree Structures in Fake Site Detection	Anti-phishing systems	Website	Machine Learning
23	2FA-PP: 2nd Factor Phishing Prevention	Anti-phishing systems	Website	Cryptography (Obfuscation)
24	A hybrid DNN–LSTM model for detecting phishing URLs	Models and Frameworks	Website	Machine Learning (DNN-LSTM)
25	A robust intelligent zero day cyberattack detection technique	Models and Frameworks	Website	Machine Learning
26	Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attack	Human-centric mitigation strategies	E-mail	Training and awareness
27	Cybersecurity of Hospitals: discussing the Challenges and Working towards Mitigating the Risks	Human-centric mitigation strategies	Generic	Recommendations and guidelines
28	Detecting Phishing SMS Based on Multiple Correlation Algorithms	Anti-phishing systems	Smishing	Machine Learning (AdaBoost Classifier)
29	Don't click: towards an effective antiphishing training. A comparative literature review	Human-centric mitigation strategies	Generic	Recommendations and guidelines

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
30	DSmishSMS-A System to Detect Smishing SMS	Models and Frameworks	Smishing	Machine Learning (Backpropagation Algorithm)
31	PenQuest: a gamified attacker/defender meta model for cyber security assessment and education	Models and Frameworks	Generic	Gamification
32	Phishing Email Detection Based on Binary Search Feature Selection	Anti-phishing systems	E-mail	Machine Learning (Binary Search Feature Selection (BSFS))
33	Social Engineering Attacks During the COVID19 Pandemic	Human-centric mitigation strategies	Generic	Recommendations and guidelines
34	The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review	Human-centric mitigation strategies	Generic	Recommendations and guidelines
35	Warning users about cyber threats through sounds	Anti-phishing systems	Website	Heuristic-based
36	A Case Study of Phishing Incident Response in an Educational Organization	Human-centric mitigation strategies	E-mail	Standard Solution
37	A Change Management Perspective to Implementing a Cyber Security Culture	Models and Frameworks	Generic	Change management
38	A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea	Models and Frameworks	Vishing	Human-centric
39	A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0	Human-centric mitigation strategies	Generic	Recommendations and guidelines
40	Alerting Users About Phishing Attacks	Human-centric mitigation strategies	Generic	Heuristic-based
41	Deep Neural Network Based Phishing Classification on a High-Risk URL Dataset	Anti-phishing systems	Website	Neural Networks (DNN)
42	Detection of phishing attacks with machine learning techniques in cognitive security architecture	Anti-phishing systems	Website	Machine Learning
43	Development of anti-phishing browser based on random forest and rule of extraction framework	Anti-phishing systems	Website	Machine Learning (Embedded Phishing Detection Browser' (EPDB))
44	Informing, simulating experience, or both: A field experiment on phishing risks	Human-centric mitigation strategies	Generic	Training and Awareness
45	Machine learning classification algorithms for adware in android devices: A comparative evaluation and analysis	Anti-phishing systems	Website	Machine Learning (RandomForest)
46	Preventing and Mitigating Ransomware: A Systematic Literature Review	Human-centric mitigation strategies	Generic	Recommendations and guidelines
47	Victim or Attacker? A Multi-dataset Domain Classification of Phishing Attacks	Anti-phishing systems	Website	Machine Learning
48	A Comparative Analysis of Machine Learning Algorithms on Malicious URL Prediction	Anti-phishing systems	Website	Machine Learning
49	A Comprehensive Survey on Identification and Analysis of Phishing Website based on Machine Learning Methods	Anti-phishing systems	Website	Machine Learning
50	A Deep Learning-Based Framework for Phishing Website Detection	Models and Frameworks	Website	Neural network (RNN-GRU model)
51	A Hybrid Security Solution for Mitigating Cyber-Attacks on Info-Communication Systems	Anti-phishing systems	Wi-Fi	Cryptography (Homomorphic technique)
52	A Model for Detecting Sounds-alike Phishing Email Contents for Persons with Visual Impairments	Models and Frameworks	E-mail	Machine Learning
53	A New Email Phishing Training Website	Human-centric mitigation strategies	E-mail	Training and Awareness
54	A Novel Method to Prevent Phishing by using OCR Technology	Anti-phishing systems	Website	Image recognition (OCR)
55	An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage	Anti-phishing systems	Website	Pseudonymization technique
56	An Intelligent System for Phishing Attack Detection and Prevention	Anti-phishing systems	Website	Machine Learning (SVM, ANN)
57	Analysis of Malicious Email Detection using Cialdini's Principles	Anti-phishing systems	E-mail	Machine Learning
58	Anti-phishing System using LSTM and CNN	Anti-phishing systems	Website	Neural network (LSTM, CNN)
59	Computer Vision Based Framework For Detecting Phishing Webpages	Models and Frameworks	Website	Machine Learning
60	Convolutional Neural Network with Character Embeddings for Malicious Web Request Detection	Anti-phishing systems	Website	Deep learning (CNN)

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
61	Cyber Intrusion Detection using Natural Language Processing on Windows Event Logs	Anti-phishing systems	Website	Deep learning and NLP
62	Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection	Anti-phishing systems	Website	Neural network (CNN, LSTM)
63	Detecting Phishing Website Using Machine Learning	Anti-phishing systems	Website	Machine Learning
64	Detection of Newly Registered Malicious Domains through Passive DNS	Anti-phishing systems	Website	Machine Learning (LightGBM)
65	Detection of Phishing URL using Bayesian Optimized SVM Classifier	Anti-phishing systems	Website	Machine Learning (SVM)
66	Detection of Phishing Websites by Using Machine Learning-Based URL Analysis	Anti-phishing systems	Website	Machine Learning
67	Different Types of Phishing Attacks and Detection Techniques: A Review	Human-centric mitigation strategies	Website	Recommendations and guidelines
68	EDITH - A Robust Framework for Prevention of Cyber Attacks in the Covid Era	Anti-phishing systems	E-mail	Generic
69	Email Anti-Phishing Detection Application	Anti-phishing systems	E-mail	Machine learning (Decision tree algorithm)
70	Generating Rules to Detect Phishing Websites Using URL Features	Models and Frameworks	Website	Data mining
71	Gravitational Search Based Feature Selection for Enhanced Phishing Websites Detection	Anti-phishing systems	Website	Machine Learning (Gravitational Search Algorithm (GSA))
72	Heuristic Phishing Detection and URL Checking Methodology Based on Scraping and Web Crawling	Anti-phishing systems	Website	Heuristic-based
73	Intelligent Phishing Url Detection: A Solution Based On Deep Learning Framework	Anti-phishing systems	Website	Neural network (Gradient boosted decision trees algorithm)
74	Machine Learning Classification Algorithms for Phishing Detection: A Comparative Appraisal and Analysis	Anti-phishing systems	Generic	Machine Learning (RandomForest)
75	Machine Learning Detection for SMiShing Frauds	Anti-phishing systems	Smishing	Machine Learning
76	Mitigating Email Phishing Attacks using Convolutional Neural Networks	Models and Frameworks	E-mail	Neural Network (CNN)
77	Naive and Neighbour Approach for Phishing Detection	Anti-phishing systems	Website	Machine Learning (KNN)
78	NoFish; Total Anti-Phishing Protection System	Anti-phishing systems	E-mail	Machine Learning and NLP
79	On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection	Models and Frameworks	Website	Machine Learning (RIPPER)
80	PhishFry - A Proactive Approach to Classify Phishing Sites Using SCIKIT Learn	Anti-phishing systems	Website	Machine Learning
81	PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System	Anti-phishing systems	Website	Machine Learning
82	Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process	Human-centric mitigation strategies	Generic	Training and Awareness
83	Phishing URL Classification Analysis Using ANN Algorithm	Anti-phishing systems	Website	Machine Learning (Random forest, ANN)
84	Phishing URL Detection via CNN and Attention-Based Hierarchical RNN	Anti-phishing systems	Website	Neural network (CNN-DL, RNN)
85	Phishing Website Classification and Detection Using Machine Learning	Models and Frameworks	Website	Machine Learning (SVM)
86	Preventive Techniques of Phishing Attacks in Networks	Human-centric mitigation strategies	Generic	Training and Awareness
87	Quick Response Code Validation and Phishing Detection Tool	Anti-phishing systems	Website	Data mining
88	Secure Suite: An Open-Source Service for Internet Security	Anti-phishing systems	Website	Deep learning
89	Social Engineering and the Dangers of Phishing	Human-centric mitigation strategies	Generic	Training and Awareness
90	SpoofCatch: A Client-Side Protection Tool Against Phishing Attacks	Anti-phishing systems	Website	Machine Learning
91	Trust me and Click! A Pilot Study of Cognitive Walkthrough for Phishing Emails	Human-centric mitigation strategies	E-mail	Human-centric
92	Verbal Deception Cue Training for the Detection of Phishing Emails	Human-centric mitigation strategies	E-mail	Training and Awareness

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
93	WC-PAD: Web Crawling based Phishing Attack Detection	Anti-phishing systems	Website	Heuristic-based
94	Zero-Day attack prevention Email Filter using Advanced Machine Learning	Anti-phishing systems	E-mail	Machine Learning
95	A Game Theoretical Model for Anticipating Email Spear-Phishing Strategies	Models and Frameworks	E-mail	Gamification
96	A HYBRID PHISHING DETECTION APPROACH FOR MOBILE APPLICATION	Anti-phishing systems	Website	Machine Learning
97	A machine learning based approach for phishing detection using hyperlinks information	Anti-phishing systems	Website	Machine Learning
98	A Mamdani Type Fuzzy Inference System to Calculate Employee Susceptibility to Phishing Attacks	Anti-phishing systems	Generic	Fuzzy logic
99	A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting	Models and Frameworks	Generic	Machine Learning (C4.5, MLP, SVM and LDA)
100	A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA)	Models and Frameworks	Generic	Neural network (DMLCA)
101	Adopting automated whitelist approach for detecting phishing attacks	Anti-phishing systems	Website	Programming
102	Agenda Pushing in Email to Thwart Phishing	Anti-phishing systems	E-mail	Programming
103	AI@ntiPhish - Machine Learning Mechanisms for Cyber-Phishing Attack	Models and Frameworks	Website	Human-centric
104	An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL	Models and Frameworks	Website	Neural Network (CNN)
105	An effective security alert mechanism for real-time phishing tweet detection on Twitter	Anti-phishing systems	Social Network	Machine Learning
106	Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection	Anti-phishing systems	Website	Programming
107	Automatic detection of phishing pages with event-based request processing, deep-hybrid feature extraction and light gradient boosted machine model	Models and Frameworks	Website	Machine Learning
108	Browser Extension based Hybrid Anti-Phishing Framework using Feature Selection	Models and Frameworks	Website	Machine Learning
109	Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)	Anti-phishing systems	E-mail	Machine Learning
110	Categorizing human phishing difficulty: a Phish Scale	Human-centric mitigation strategies	E-mail	Training and Awareness
111	Detecting E-Banking Phishing Website using C4.5 Algorithm	Models and Frameworks	Website	Data mining
112	Detecting Internet of Things attacks using distributed deep learning	Models and Frameworks	Website	Machine Learning (CNN)
113	Detecting phishing attacks using a combined model of LSTM and CNN	Models and Frameworks	Website	Machine Learning (LSTM and CNN)
114	Detection of Phishing in Internet of Things Using Machine Learning Approach	Anti-phishing systems	Generic	Machine Learning (random forest classifier, support vector machine, and logistic regression)
115	Detection of phishing websites using an efficient feature-based machine learning framework	Anti-phishing systems	Website	Machine Learning
116	Detection Technique and Mitigation Against a Phishing Attack	Anti-phishing systems	Website	Programming
117	Domain Classifier: Compromised Machines Versus Malicious Registrations	Anti-phishing systems	Website	Machine Learning
118	Don't Forget the Human: a Crowdsourced Approach to Automate Response and Containment Against Spear Phishing Attacks	Human-centric mitigation strategies	Generic	Training and Awareness
119	Enterprise Credential Spear-phishing attack detection	Anti-phishing systems	E-mail	Programming
120	HinPhish: An Effective Phishing Detection Approach Based on Heterogeneous Information Networks	Anti-phishing systems	Website	Machine Learning
121	Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach	Anti-phishing systems	Generic	Training and Awareness

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
122	Improving Phishing Awareness in the United States Department of Defense	Anti-phishing systems	Generic	Training and Awareness
123	Increasing Protection against Internet Attacks through Contextual Feature Pairing	Anti-phishing systems	Website	Machine Learning
124	Intelligent Association Classification Technique for Phishing Website Detection	Models and Frameworks	Website	Machine Learning
125	Intelligent Ensemble Learning Approach for Phishing Website Detection Based on Weighted Soft Voting	Anti-phishing systems	Website	Machine Learning
126	Intelligent phishing detection scheme using deep learning algorithms	Anti-phishing systems	Website	Machine Learning (LSTM and CNN)
127	Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text	Anti-phishing systems	Generic	Fuzzy logic
128	LogoSENSE: A companion HOG based logo detection scheme for phishing web page and E-mail brand recognition	Models and Frameworks	Website	Machine Learning (SVM classifier, Histogram of Oriented Gradients HOG)
129	Machine Learning-Based Malicious X.509 Certificates' Detection	Anti-phishing systems	Website	Machine Learning
130	Malicious URL Detection based on Machine Learning	Anti-phishing systems	Website	Machine Learning
131	New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing	Models and Frameworks	Generic	Cryptography
132	On detecting and mitigating phishing attacks through featureless machine learning techniques	Anti-phishing systems	Website	Machine Learning
133	Online meta-learning firewall to prevent phishing attacks	Anti-phishing systems	Generic	Machine Learning
134	Phishing Email Detection based on Named Entity Recognition	Models and Frameworks	E-mail	Machine Learning
135	Phishing in healthcare organisations: threats, mitigation and approaches	Human-centric mitigation strategies	Generic	Training and Awareness
136	Phishing page detection via learning classifiers from page layout feature	Anti-phishing systems	Generic	Machine Learning
137	Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning	Models and Frameworks	Website	Neural network
138	Phishing Website Detection: Forest by Penalizing Attributes Algorithm and Its Enhanced Variations	Models and Frameworks	Website	Machine Learning
139	Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages	Models and Frameworks	Website	Neural network
140	Privacy Preserving Machine Learning for Malicious URL Detection	Anti-phishing systems	Website	Machine Learning
141	Privacy-aware detection framework to mitigate new-age phishing attacks	Human-centric mitigation strategies	Website	Training and Awareness
142	Proactive Detection of Phishing Kit Traffic	Models and Frameworks	E-mail	Neural Network
143	Rotation Forest-Based Logistic Model Tree for Website Phishing Detection	Models and Frameworks	Generic	Machine Learning
144	Secure Real-Time Computational Intelligence System Against Malicious QR Code Links	Anti-phishing systems	Website	Machine Learning
145	Social Engineering Attacks: Recent Advances and Challenges	Human-centric mitigation strategies	Generic	Generic
146	Tear Off Your Disguise: Phishing Website Detection Using Visual and Network Identities	Anti-phishing systems	Website	Machine Learning
147	Towards benchmark datasets for machine learning based website phishing detection: An experimental study	Human-centric mitigation strategies	Website	Machine Learning
148	Unified Payment Interface (UPI) platform: Conniving tool for Social Engineering Attack	Anti-phishing systems	Generic	Programming
149	VPCID-A VoIP Phone Call Identification Database	Anti-phishing systems	Vishing	Machine Learning
150	Rapid Homoglyph Prediction and Detection	Anti-phishing systems	Website	Machine Learning
151	Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking	Anti-phishing systems	E-mail	Software Defined Networks
152	Studying user's computer security behaviour in developing an effective antiphishing educational framework	Human-centric mitigation strategies	Generic	Training and Awareness
153	Improving Email Security with Fuzzy Rules	Anti-phishing systems	E-mail	Fuzzy logic

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
154	Countermeasure Against Spoofed E-mails Using Display Name as a User Authenticator	Anti-phishing systems	E-mail	Programming
155	MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook	Models and Frameworks	Social Network	Machine Learning
156	Effective Phishing Website Detection Based on Improved BP Neural Network and Dual Feature Evaluation	Models and Frameworks	E-mail	Neural network
157	An Effective Neural Network Phishing Detection Model Based on Optimal Feature Selection	Models and Frameworks	Website	Neural network
158	Improving Phishing Detection with the Grey Wolf Optimizer	Models and Frameworks	Generic	Machine Learning (a multi-objective grey wolf optimizer)
159	PDGAN: Phishing Detection With Generative Adversarial Networks	Models and Frameworks	Website	Deep learning (LSTM, CNN)
160	Phishing Detection and Prevention using Chrome Extension	Anti-phishing systems	Website	Programming
161	ADVERT: An Adaptive and Data-Driven Attention Enhancement Mechanism for Phishing Prevention	Anti-phishing systems	E-mail	Real-time visual aids
162	Metaheuristic Optimization of Neural Networks for Phishing Detection	Anti-phishing systems	Website	Neural network
163	Combining Long-Term Recurrent Convolutional and Graph Convolutional Networks to Detect Phishing Sites Using URL and HTML	Anti-phishing systems	Website	Machine Learning
164	Detect Phishing Website by Fuzzy Multi-Criteria Decision Making	Anti-phishing systems	Website	Fuzzy logic
165	CatchPhish: Model for detecting homographic attacks on phishing pages	Models and Frameworks	Website	Machine Learning
166	Web Extension for Phishing URL Identification	Anti-phishing systems	Website	Programming
167	CNN based Prediction Analysis for Web Phishing Prevention	Models and Frameworks	E-mail	Machine Learning (OMCFS, CNN)
168	Eth-PSD: A Machine Learning-Based Phishing Scam Detection Approach in Ethereum	Anti-phishing systems	Generic	Machine Learning
169	Autoencoder-Based Feature Selection for Phishing URL Attack Detection in IoT Using Stacked Autoencoder (AFS-SAE)	Models and Frameworks	Website	Machine Learning
170	Korean Dialect Identification Based on an Ensemble of Prosodic and Segmental Feature Learning for Forensic Speaker Profiling	Models and Frameworks	Vishing	Machine Learning
171	Prevention of Phishing attacks using AI Algorithm	Models and Frameworks	Website	Machine Learning (LTSM)
172	On Phishing: Proposing a Traffic Behavior-Based Model to Detect, Prevent, and Classify Webpage Suspicious and Malicious Activities	Models and Frameworks	Website	Machine Learning
173	Phishing Attack Mitigation Using Convolutional Neural Networks	Models and Frameworks	Website	Machine Learning (CNN)
174	Phish-Sight: a new approach for phishing detection using dominant colors on web pages and machine learning	Anti-phishing systems	Website	Machine Learning
175	PhishSim: Aiding Phishing Website Detection With a Feature-Free Tool	Anti-phishing systems	Website	Machine Learning
176	PhishSpy - A Phishing Detection Tool and Defensive Approaches	Anti-phishing systems	Website	Machine Learning
177	Profiler: Distributed Model to Detect Phishing	Models and Frameworks	E-mail	Machine Learning
178	Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioral Intentions About Phishing	Human-centric mitigation strategies	Generic	Training and Awareness
179	A deep learning model with hierarchical LSTMs and supervised attention for anti-phishing	Models and Frameworks	E-mail	Neural network
180	A machine learning approach for detecting fast flux phishing hostnames	Models and Frameworks	Generic	Machine Learning
181	A Machine-Learning Based Approach for Detecting Phishing URLs	Models and Frameworks	E-mail	Machine Learning (XGBoost classifier and the random forest)

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
182	A novel approach for phishing emails real time classification using k-means algorithm	Models and Frameworks	E-mail	Machine Learning (K-means algorithm)
183	A Proposal Phishing Attack detection System on Twitter	Anti-phishing systems	Social Network	Machine Learning (MLP)
184	A Training Web Platform to Improve Cognitive Skills for Phishing Attacks Detection	Human-centric mitigation strategies	Generic	Training and Awareness
185	A visualization cybersecurity method based on features' dissimilarity	Models and Frameworks	Website	Fuzzy logic
186	An Enhanced Phishing Detection Tool Using Deep Learning From URL	Anti-phishing systems	Website	Deep learning
187	Anti-phishing model based on relative content mining	Models and Frameworks	Website	Machine learning (Relative Content Mining)
188	ASPA-MOSN: An Efficient User Authentication Scheme for Phishing Attack Detection in Mobile Online Social Networks	Anti-phishing systems	Social Network	Cryptography
189	Boosting Guided Probabilistic Ensemble-based Approach For Phishing Website Detection	Anti-phishing systems	Website	Machine Learning (Probabilistic ensemble-based integrated solution)
190	Classification of Phishing Email Using Word Embedding and Machine Learning Techniques	Anti-phishing systems	E-mail	Machine Learning (Random Forest)
191	CNN-Fusion: An effective and lightweight phishing detection method based on multi-variant ConvNet	Anti-phishing systems	Website	Deep learning (CNN)
192	Deep learning in phishing mitigation: a uniform resource locator-based predictive model	Models and Frameworks	E-mail	Deep learning (CNN-BiLSTM)
193	DeepAnti-PhishNet: Applying deep neural networks for phishing email detection CEN-AISecurity@IWSPA-2018	Anti-phishing systems	E-mail	Deep learning (CNN, RNN)
194	Detecting Phishing Websites Using Neural Network and Bayes Classifier	Anti-phishing systems	Website	Neural network
195	Detection of online phishing email using dynamic evolving neural network based on reinforcement learning	Models and Frameworks	E-mail	Neural network
196	Detection of Phishing Websites Using Classification Algorithms	Anti-phishing systems	Website	Machine Learning
197	Detection of phishing websites using data mining tools and techniques	Anti-phishing systems	Website	Data mining
198	EBONN: AN ENHANCED BAYESIAN OPTIMIZED NEURAL NETWORK FOR CLASSIFICATION OF PHISHING ATTACKS	Anti-phishing systems	Website	Neural network
199	Employing cluster-based class decomposition approach to detect phishing websites using machine learning classifiers	Anti-phishing systems	Website	Machine Learning (Decision tree algorithm, Random Forest)
200	Evolutionary Algorithm with Deep Auto Encoder Network Based Website Phishing Detection and Classification	Models and Frameworks	Website	Machine Learning
201	HearMeOut: Detecting Voice Phishing Activities in Android	Anti-phishing systems	Vishing	Machine Learning
202	Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach	Anti-phishing systems	Website	Deep Learning
203	Intelligent Phishing Website Detection Using Deep Learning	Models and Frameworks	Website	Deep Learning
204	Intelligent phishing website detection using machine learning	Models and Frameworks	Website	Machine Learning
205	Machine learning based phishing E-mail detection Security-CEN@Amrita	Models and Frameworks	E-mail	Machine Learning
206	Nophish: A phish detector in cloud services	Models and Frameworks	Website	Machine Learning (SVM)
207	Phish Block: A Blockchain Framework for Phish Detection in Cloud	Models and Frameworks	Website	Blockchain
208	PhishBox: An approach for phishing validation and detection	Models and Frameworks	Website	Machine Learning
209	PhishGuard-An Automatic Web Phishing Detection System	Anti-phishing systems	Generic	Machine Learning
210	Phishing Detection System through Hybrid Machine Learning Based on URL	Models and Frameworks	E-mail	Machine Learning
211	Phishing Site Detection Using Artificial Intelligence	Models and Frameworks	Website	Machine Learning
212	PHISHING URL DETECTION USING LSTM BASED ENSEMBLE LEARNING APPROACHES	Models and Frameworks	Website	Machine Learning (LSTM)
213	Applying machine learning techniques to detect and analyze web phishing attacks	Models and Frameworks	Website	Machine Learning

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
214	Kn0w Thy Doma1n Name: Unbiased Phishing Detection Using Domain Name Based Features	Models and Frameworks	Website	Machine Learning
215	Leveraging Deep Learning Image Classifiers for Visual Similarity-Based Phishing Website Detection	Models and Frameworks	Website	Machine Learning
216	Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild	Anti-phishing systems	Website	Machine Learning
217	Phishing E-Mail Detection by Using Deep Learning Algorithms	Anti-phishing systems	E-mail	Deep learning
218	Phishing URL Detection: A Network-Based Approach Robust to Evasion	Models and Frameworks	Website	Machine Learning
219	Phishing Website Detection Using Deep Learning	Anti-phishing systems	Website	Deep learning
220	PHISHWEB: A Progressive, Multi-Layered System for Phishing Websites Detection	Anti-phishing systems	Website	Machine Learning
221	Segmentation-Based Phishing URL Detection	Anti-phishing systems	E-mail	Natural Language Processing
222	SoK: Human-Centered Phishing Susceptibility	Human-centric mitigation strategies	Generic	Recommendations and guidelines
223	“Alexa, What’s a Phishing Email?”: Training users to spot phishing emails using a voice assistant	Human-centric mitigation strategies	Generic	Training and Awareness
224	A human-centred design approach for the development and conducting of maritime cyber resilience training	Human-centric mitigation strategies	Generic	Training and Awareness
225	Cloud-based email phishing attack using machine and deep learning algorithm	Anti-phishing systems	E-mail	Machine Learning and Deep learning
226	Deep convolutional forest: a dynamic deep ensemble approach for spam detection in text	Anti-phishing systems	Website	Machine Learning
227	DomainObserver: A Lightweight Solution for Detecting Malicious Domains Based on Dynamic Time Warping	Anti-phishing systems	Website	Machine Learning
228	Implementation of ‘Smishing Detector’: An Efficient Model for Smishing Detection Using Neural Network	Models and Frameworks	Smishing	Neural network
229	Phish-Pharm: A Searchable Database of Pharmacokinetics and Drug Residue Literature in Fish — 2022 Update	Models and Frameworks	Generic	Generic
230	Piracema: a Phishing snapshot database for building dataset features	Models and Frameworks	Generic	Machine Learning
231	Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours	Human-centric mitigation strategies	Generic	Training and Awareness
232	SMILE - Smart eMail Link Domain Extractor	Anti-phishing systems	Website	Programming
233	TFC: Defending Against SMS Fraud via a Two-Stage Algorithm	Anti-phishing systems	Smishing	Machine Learning
234	Phish Responder: A Hybrid Machine Learning Approach to Detect Phishing and Spam Emails	Anti-phishing systems	E-mail	Machine Learning
235	PhishNot: A Cloud-Based Machine-Learning Approach to Phishing URL Detection	Anti-phishing systems	Website	Machine Learning
236	Prevention and mitigation measures against phishing emails: a sequential schema model	Models and Frameworks	E-mail	Machine Learning
237	Prevention of Phishing Attacks Using QR Code Safe Authentication	Anti-phishing systems	Website	Cryptography
238	RAIDER: Reinforcement-Aided Spear Phishing Detector	Anti-phishing systems	E-mail	Reinforcement learning
239	Visual similarity-based phishing detection using deep learning	Anti-phishing systems	Website	Deep learning
240	A content and URL analysis-based efficient approach to detect smishing SMS in intelligent systems	Anti-phishing systems	Smishing	Machine Learning
241	A new method for Detection of Phishing Websites: URL Detection	Anti-phishing systems	Website	Machine Learning
242	An effective detection approach for phishing websites using URL and HTML features	Anti-phishing systems	Website	Machine Learning
243	An Improved Ensemble Deep Learning Model Based on CNN for Malicious Website Detection	Models and Frameworks	Website	Machine Learning (CNN, BiGRU)
244	AntiPhiMBS-TRN: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Transaction Level	Models and Frameworks	Generic	Process metalanguage (PROMELA)

(*continued on next page*)

(*continued*)

S. No.	Name of the publication	Classification	Targeted Phishing vector	Underlying concept/ methodology
245	APuML: An Efficient Approach to Detect Mobile Phishing Webpages using Machine Learning	Anti-phishing systems	Website	Machine Learning
246	C-R-P-M-I: A Framework to Model Cyber-Risk from Phishing and Mitigation through Cyber Insurance Emergent Research Forum (ERF)	Models and Frameworks	Generic	Machine Learning
247	DeepDetection: Privacy-Enhanced Deep Voice Detection and User Authentication for Preventing Voice Phishing	Anti-phishing systems	Vishing	Programming
248	HELPHED: Hybrid Ensemble Learning Phishing Email Detection	Models and Frameworks	E-mail	Machine Learning

References

Abdillah, R., Shukur, Z., Mohd, M., Murah, M.Z., 2022. Phishing classification techniques: a systematic literature review. IEEE Access 10, 41574–41591.

Adriaanse, S., Rensleigh, C., 2013. Web of Science, Scopus, and Google Scholar: a content comprehensiveness comparison. Electr. Lib. 31 (6), 727–744.

Alauthman, M., Almomani, A., Alweshah, M., Omoush, W., Alieyan, K., 2019. Machine learning for phishing detection and mitigation. In: Machine Learning for Computer and Cyber Security. CRC Press, pp. 48–74.

Althobaiti, K., Jenkins, A.D.G., Vaniea, K., 2021. A case study of phishing incident response in an educational organization. Proc. ACM Hum.-Comput. Interact. 5 (CSCW2), 1–32. doi:10.1145/3476079.

Apandi, S.H., Sallim, J., Sidek, R.M., 2020. 'Types of anti-phishing solutions for phishing attack. IOP Conf. Ser.: Mater. Sci. Eng. 769, 012072.

Argaw, S.T., et al., 2019. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med. Inf. Decis. Making 19 (1), 10. doi:10.1186/s12911-018-0724-5.

Argaw, S.T., et al., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med. Inf. Decis. Making 20 (1), 146. doi:10.1186/s12911-020-01161-7.

Arshad, A., Rehman, A.U., Javaid, S., Ali, T.M., Sheikh, J.A., Azeem, M., 2021. A systematic literature review on phishing and anti-phishing techniques. Pakistan J. Eng. Tech. 4 (1), 163–168.

Babati, B., (2020). How human error impacts human risk in cybersecurity? Available: https://www.hoxhunt.com/blog/human-error-impacts-human-risk-in-cybersecurity.

Benavides, E., Fuertes, W., Sanchez, S., Sanchez, M., 2020. In: Rocha, Á., Pereira, R. (Eds.). In: Developments and Advances in Defense and Security, 152. Smart Innovation, Systems and Technologies, Singapore, pp. 51–64.

Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M., 2007. Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Softw. 80 (4), 571–583.

Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., Shukla, S., 2022. Applications of deep learning for phishing detection: a systematic literature review. Knowl. Inf. Syst. 64 (6), 1457–1500.

Chanti, S., Chithralekha, T., 2020. Classification of anti-phishing solutions. SN Comput. Sci. 1, 11. doi:10.1007/s42979-019-0011-2.

Chen, Y.-H., Chen, J.-L., 2019. AI@ntiPhish — Machine Learning Mechanisms for Cyber-Phishing Attack. IEICE. Trans. Inf. Syst. E102.D (5), 878–887. doi:10.1587/transinf.2018NTI0001.

Chiew, K.L., Yong, K.L.C, Tan, C.L., 2018. A survey of phishing attacks: their types, vectors, and technical approaches. Expert Syst. Appl. 106 (2018), 1–20.

Dam, L. and Deshpande, K. (2021) 'Unified Payment Interface (UPI) platform: Conniving tool for Social Engineering Attack', pp. 17–28.

Das, S., Kim, A., Tingle, Z. and Nippert-Eng, C. (2019). All about phishing: Exploring user research through a systematic literature review. arXiv preprint arXiv:1908.05897.

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T., Costabile, M.F., 2021. Human factors in phishing attacks: a systematic literature review. ACM Comput. Surv. (CSUR) 54 (8), 1–35.

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., Guizani, M., 2017. Systematization of knowledge (sok): a systematic review of software-based web phishing detection. IEEE Commun. Surv. Tutor. 19 (4), 2797–2819.

Drichel, A., Drury, V., von Brandt, J. and Meyer, U., 2021. Finding phish in a haystack: A pipeline for phishing classification on certificate transparency logs. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-12).

Dukarm, C., Dill, R., Reith, M., 2019. Improving phishing awareness in the united states department of defense. In: Cruz, T., Simoes, P. (Eds.), Proceedings of the 18th European Conference on Cyber Warfare and Security (2019), Nr Reading: Acad Conferences Ltd, pp. 172–177 Available at:.

Ellis, D. (2023),' 7 Ways to Recognize a Phishing Email: Email Phishing Examples'. Available at: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email.

Falagas, M.E., Pitsouni, E.I., Malietzis, G.A., Pappas, G., 2008. Comparison of PubMed, Scopus, web of science, and Google scholar: strengths and weaknesses. FASEB J. 22 (2), 338–342.

Farooq, A., Feizollah, A., & ur Rehman, M.H. (2021). Federated learning research: trends and bibliometric analysis. Federated Learning Systems: Towards Next-Generation AI, 1-19.

IBM. (2022). Cost of a Data Breach Report 2022, Available at: https://www.ibm.com/sg-en/security/data-breach.

Jampen, D., et al., 2020. 'Don't click: towards an effective anti-phishing training. A comparative literature review. Hum.-Centric Comput. Inf. Sci. 10 (1), 33. doi:10.1186/s13673-020-00237-7.

Kitchenham, B., 2004. In: Procedures for performing systematic reviews, 33. Keele University, Keele, UK, pp. 1–26.

Kitchenham, B., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering: Technical Report EBSE-2007-01. Software Engineering Group, Keele University.

Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S., 2009. Systematic literature reviews in software engineering–a systematic literature review. Inf. Softw. Technol. 51 (1), 7–15.

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O.P., Turner, M., Niazi, M., Linkman, S., 2010. Systematic literature reviews in software engineering–a tertiary study. Inf. Softw. Technol. 52 (8), 792–805.

Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of literature. Crime Sci. 3 (1), 1–10.

Lim, J., Zhou, L., Zhang, D. Verbal Deception Cue Training for the Detection of Phishing Emails. IEEE International Conference on Intelligence and Security Informatics (ISI). 2021, pp. 1-3, doi: 10.1109/ISI53945.2021.9624738.

Manjezi, Z. and Botha, R. (2018) 'Preventing and Mitigating Ransomware - a Systematic Literature Review', in ISSA. doi:10.1007/978-3-030-11407-7_11.

Mashtalyar, N., Ntaganzwa, U., Santos, T., Hakak, S., Ray, S., 2021. Social Engineering Attacks: recent Advances and Challenges. HCI for Cybersecurity, Privacy and Trust 417–431.

MiInsbridge (2023), '5 Characteristics of a Phishing Email'. Available at: https://www.milnsbridge.com.au/5-characteristics-phishing-email/.

Moul, K.A., 2019. Avoid Phishing Traps. In: Proceedings of the 2019 ACM SIGUCCS Annual Conference, New York, NY, USA: Association for Computing Machinery (SIGUCCS '19), pp. 199–208. doi:10.1145/3347709.3347774.

Ozcan, A., Catal, C., Donmez, E., Senturk, B., 2021. 'A hybrid DNN–LSTM model for detecting phishing URLs'. Neural Comput. Appl. 1–17.

Ponemon Institute. (2021). The 2021 Cost of Phishing Study. Available at: https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-ponemon-2021-cost-of-phishing-study.pdf.

Priestman, W., et al., 2019. Phishing in healthcare organizations: threats, mitigation and approaches. BMJ Health Care Inf. 26. doi:10.1136/bmjhci-2019-100031.

Sadiq, A., et al., 2021. A review of phishing attacks and countermeasures for the internet of things-based smart business applications in industry 4.0. Hum. Behav. Emerg. Technol. 3 (5), 854–864. doi:10.1002/hbe2.301.

Safi, A., Singh, S., 2023. A Systematic Literature Review on Phishing Website Detection Techniques. Journal of King Saud University-Computer and Information Sciences.

Salloum, S., Gaber, T., Vadera, S., Sharan, K., 2022. A systematic literature review on phishing email detection using natural language processing techniques. IEEE Access.

Sameen, M., Han, K., Hwang, S.O., 2020. PhishHaven—an Efficient Real-Time AI Phishing URLs Detection System. IEEE Access 8, 83425–83443. doi:10.1109/ACCESS.2020.2991403.

Valente, A., Holanda, M., Mariano, A.M., Furuta, R., Da Silva, D., 2022. Analysis of Academic Databases for Literature Review in the Computer Science Education Field. In: 2022 IEEE Frontiers in Education Conference (FIE), IEEE, pp. 1–7.

Valentim, R., Drago, I., Trevisan, M., Cerutti, F. and Mellia, M., (2021) 'Augmenting phishing squatting detection with GANs' In Proceedings of the CoNEXT Student Workshop (pp. 3-4).

Venkatesha, S., Reddy, K.R., Chandavarkar, B.R., 2021. Social engineering attacks during the COVID-19 pandemic. SN Comput. Sci. 2 (2), 78. doi:10.1007/s42979-020-00443-1.

Verizon. (2022). Data Breach Investigations Report (DBIR). Available at: https://www.verizon.com/business/resources/T920/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

Wash, R., 2020. How experts detect phishing scam emails. Proc. ACM Hum.-Comput. Interact. 4 (CSCW2), 1–28. doi:10.1145/3415231.

Younis, A. and Musbah, M. (2020) A framework to protect against phishing attacks. doi:10.1145/3410352.3410825.

Bilal Naqvi is a post-doctoral researcher at LUT University, Finland. He received Ph.D. from LUT University, Finland. His main research interests include human aspects of security and security implications of digitalization schemes. Previously he has received B.E. degree in computer software engineering and the M.S. degree in information security from the National University of Sciences and Technology, NUST, Pakistan.

Kseniia Perova is a doctoral student working at LUT University, Finland. Ksenia's completed her master's in software engineering and Digital Transformation and has special interest in cyber security issues.

Dr. Ali Farooq is a Senior Research Consultant at Qatar Computing Research Institute, Doha, Qatar, and a visiting researcher at the Department of Computing, University of Turku, Finland. He holds a D.Sc.(Tech.) and MSc.(Tech.) degrees in ICT from the University of Turku. He also holds a Commonwealth executive MBA. His research focus is on "where human meets technology", especially security and privacy behaviors and their outcomes, including wellbeing. His other areas of interest are the dark side of technology and improving the learning and engagement of the future and existing workforce.

Imran Makhdoom is a postdoc researcher at the University of Technology Sydney. He completed his Ph.D. from the University of Technology Sydney in 2020. His research interests include blockchain, the Internet of Things, distributed consensus, network, and computer security. Imran has published numerous papers in some of the prestigious journals and conferences. He has also been a Food Agility Scholar from 2019 to 2020 and has made a valuable contribution to data security and privacy in the Food Tech/Agri Tech. Before this, he secured a master's degree in information security from the National University of Sciences and Technology, Pakistan, in 2015.

Shola Oyedeji is a postdoctoral researcher at LUT University Finland with research on software sustainability by design focused on integrating the human, societal, environmental, technical and economic concerns into software systems design and measurement to support sustainability. He is also a postdoctoral researcher fellow at University L'Aquila, Italy with research on Identifying and prioritizing sustainability concerns of companies to software design.

Jari Porras D.Sc (Tech) is Professor of Software Engineering (especially Distributed Systems) at the Lappeenranta-Lahti University of Technology LUT. Prof. Porras received the DSc. (Tech.) degree from the Lappeenranta University of Technology, Finland in 1998 about modeling and simulation of communication networks in distributed computing environment. He has supervised approx. 500 Master's Thesis works and 22 Dissertations as well as acted as external evaluator for 21 doctoral thesis works since the start of his professorship. He has conducted research on parallel and distributed computing, wireless and mobile systems, and services as well as sustainable ICT. In last years he has focused his research on human and sustainability aspects of software engineering. He is actively working in international networks and organizations.