CREATING GUIDELINES AND BEST PRACTICES AGAINST PHISHING AND RANSOMWARE ATTACKS FOR HEALTHCARE PERSONNEL

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Science

Master's Degree Programme in Software Engineering and Digital transformation

2022

Kseniia Perova

Examiners: Professor Jari Porras, D.Sc (Tech), LUT University

Dr. Bilal Naqvi, Ph.D, LUT University

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

School: LUT School of Engineering Science

Degree Programme in Software Engineering and Digital transformation

Kseniia Perova

Creating Guidelines and Best Practices against Phishing and Ransomware Attacks for Healthcare Personnel

Master's thesis

2022

87 pages, 17 figures, 10 tables and 1 appendix

Examiners: Professor Jari Porras and Dr. Bilal Naqvi

Keywords: phishing, guidelines, best practices, tools, prevention techniques, prevention, mitigation, solutions, healthcare.

Amidst the digitalization of services across all sectors, it is essential to stay up to date with the protection mechanisms to be able to protect the systems and services against a multitude of cyber-attacks. Cyber-attacks can have even more severer consequences in the domain of healthcare, as in the case of a cyber-attack on healthcare infrastructures and services, the impact is not limited to material aspects, but human lives are also endangered. Among the most prevalent cyber-attacks are phishing and ransomware attacks. During the thesis, existing mitigation approaches against these attacks were explored. The key contributions of this thesis include: (1) identification of existing mechanisms and guidelines against phishing and ransomware attacks from the existing literature by means of a systematic literature review, (2) lists of guidelines and recommendations to protect against phishing and ransomware attacks, and (3) extending the scope of SLR by proposing a methodology for conducting co-design workshop with industry representatives to capturing more state-of-the-art guidelines and best practices.

ABBREVIATIONS

SLR	Systematic Literature Review
PR	Participatory Research
ICT	Information and Communications Technology
MFA	Microsoft Multi-Factor Authentication
SRHD	Spokane Regional Health District
VPN	Virtual Private Network
BEC	Business Email Compromise

Table of contents

Appendices

Appendix 1. The empirical data from articles

1. Introduction

Digital transformation is a modern trend affecting various sectors. Organizations seek innovative solutions and ideas to maintain their competitiveness and share of the market. The transformation to a digital society requires a change in business processes and industrial companies, as well as changes in the activities of a business and financial institutions. (Kraus et al., 2021).

The coronavirus pandemic has accelerated the digital transformation taking place in healthcare, and both patients and service providers have seen the benefits of new technologies and virtual solutions. The healthcare sector is also using modern ICT systems for patient records, telemedicine meetings, remote patient monitoring services, and modified insurance offers.

Digital technologies for healthcare have a profound impact on how medical services are provided, from technology that can better manage health services to better diagnosis and monitoring the effects of policies on public health. The wave of digitization has created many opportunities to improve existing infrastructures and has made it possible to provide quality medical care to consumers faster and cheaper (Intelligence, 2022).

One aspect that needs to be clarified is why the healthcare sector was considered during this thesis. This is explained by the fact that the health sector in 2019 accounted for the highest health expenditure compared to GDP among the EU Member States. For instance, Germany has 11.7 percent and France has 11.1 percent (Eurostat, 2021). Ensuring that people and societies are protected from social health hazards and have an equal opportunity for quality health care has a major positive impact on the health, economic growth, and development of citizens and society. The health sector is also an important employment sector and has significant potential for employment creation. Digital transformation brings new possibilities for providing better medical treatment.

However, the ability of attackers to extract medical data has increased significantly due to the transition to online provision of medical services, remote e-health, and telemedicine

(ENISA, 2021). The past decade witnessed an increase in cyber-attacks (Accenture, 2021). With the digitization of services, cyber-attacks on systems and services could hamper all the benefits of digitization. Moreover, the recent trends show that cyber-attacks targeted at humans are increasing. According to the IBM Cyber Security Intelligence Index 2014, 95 percent of security incidents in 2014 were due to human error (IBM, 2014). Among these prevalent attacks targeted at human users, the most common are phishing attacks. Phishing is an attack aimed at imitating the official websites of companies such as banks, electronic commerce, and government agencies. Phishing attacks could be more consequential when they are used as a vector to launch ransomware attacks. Ransomware attacks are types of malicious attacks that encrypt data in organizations and demand payment to restore access (IBM, 2022). The first ransomware attack occurred in 1989 and was related to healthcare (Becker's Healthcare, 2016). The frequency and complexity of ransomware attacks have increased by more than 150 percent in 2020 and have become one of the most serious threats faced by companies today, regardless of the sector to which they belong (IBM, 2022). This attack is especially dangerous because it can restrict access to the system. Ransomware attacks often target the healthcare infrastructure due to their criticality. Therefore, the main goal of the thesis is to create guidelines and best practices against phishing and ransomware attacks on healthcare personnel.

1.1 Research objectives and questions

The thesis considers the following principal research question:

- *What are the prevention mechanisms against phishing and ransomware attacks?*

The following sub-research questions helped answer the main research question:

1. What are the prevention mechanisms reported in the literature?
2. How can the existing solutions be classified and visually represented?
3. Is there a way to supplement the recommendations from the literature?

The objectives of the thesis include the following.

1. To discuss the importance of preventing phishing and ransomware attacks.
2. To conduct a systematic literature review (SLR) to identify guidelines and best practices from the existing literature on how to prevent phishing and ransomware attacks.

3. To develop recommendations for protecting against phishing attacks and ransomware.
4. To propose a methodology for a co-design workshop with representatives from the cyber-security industry to synthesize new knowledge on how to prevent phishing and ransomware attacks.

1.2 Research method

The thesis is mainly focused on a Systematic Literature Review (SLR). In addition, this research proposed a co-design approach, which is built upon Participatory Research (PR).

A systematic literature review is a systematic process of collecting and critically analyzing several research papers. Co-design is a process guided by design using creative and participatory methods. Co-design is a participatory approach to solving problems that treat community members as equal collaborators in the design process.

The reason for combing the two research methods is to synthesize findings from SLR and suggestions from co-design workshop attendees. The idea is to discuss with participants of the future workshop the SLR results and modify them according to people's experiences. However, before planning the co-design stage, it is essential to search for existing methods beforehand for successfully conducting the co-design workshop. This will be outlined in the thesis.

1.3 Phases of the research

The research process consists of 5 phases: (i) planning phase, (ii) conceptual phase, (iii) analysis phase, (iv) development phase, and (v) reporting phase.

(i) Planning phase

This phase included the identification of research tasks and evaluation of project execution time. Figure 1 illustrates the estimated time for each phase using a Gantt chart.

	Task Name	Duration	Start	Finish
1	Master thesis project	85 days	01.02.22	1.05.22
2	Conceptual phase	42 days	01.02.22	15.03.22
3	Problem analysis	28 days	01.02.22	28.02.22
4	Conducting Systematic Literature review	13 days	1.03.22	13.03.22
5	Exploring a co-design workshop method	1 day	14.03.22	15.03.22
9	Analytic phase	21 days	16.03.22	7.03.22
8	Analyzing data from SLR resources	21 day	16.03.22	7.04.22
9	Development phase	7 days	08.04.22	14.04.22
10	Developing the outline for conducting a workshop	4 days	08.04.22	11.04.22
11	Propose activities for a co-design workshop	3 days	12.04.22	14.04.22
16	Reporting phase	15 days	15.04.22	1.05.22
17	Preparation of master thesis report	7 days	15.04.22	22.04.22
18	Correction of report	8 days	23.04.22	30.04.22
19	Upload of report	0 days	1.05.22	1.05.22

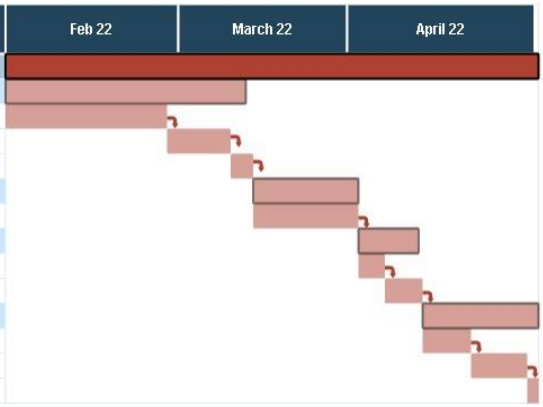

Figure 1. Planning phases of the research.

(ii) Conceptual phase

This phase constituted of the following tasks:

1. Problem analysis: the analysis of the current situation with cyber-attacks.
2. Solution method: description of the whole methodology of the research.
3. Systematic Literature Review: collecting information from different sources with related topics from chosen databases for conducting the SLR.Co-design approach: exploring the idea of a co-design workshop and its methods.

(iii) Analysis phase

Analyzing data from SLR resources. The relevant data will be found after conducting a systematic literature review. Some insights will be used for conducting a co-design workshop.

(iv) Development phase

To synthesize the data about existing solutions. To formulate recommendations and visualize them. Developing the outline for conducting a co-design workshop. Propose activities for conducting a co-design workshop.

(v) Reporting phase

All the collected data, including literature review, research results, proposed methods for a co-design workshop, and conclusions, are presented in this thesis.

1.4 Structure of the thesis

The SLR is a necessity to summarize empirical data from various sources on existing solutions from the perspective of specialists in different fields and data reports. Assumed from the reviews of these articles, a theoretical framework has been created for cybersecurity companies and industries interested in gaining knowledge about cyber threat prevention methods. The thesis begins with a description of existing cyber-attacks, discussing the principles of their work, the examples of attacks, and their impact and main threats. The SLR is implemented to analyze methods for combating phishing and ransomware attacks. The results are systematized and contain empirical data. In the results chapter, a list of guidelines and recommendations to protect against phishing and ransomware attacks is proposed. Moreover, based on the results, suggestions for conducting a co-design workshop with representatives from cybersecurity companies are presented. In conclusion, possible limitations and future research directions are identified.

1.5 Outcomes

This thesis aims to create guidelines and approaches for preventing cyber-attacks in the healthcare sector by identifying existing solutions proposed in the existing literature. These solutions were identified through a systematic literature review (SLR). By the end of the work, suggestions for conducting a co-design workshop were created. In terms of positively influencing the abilities of healthcare personnel in detecting, reporting, and mitigating phishing and ransomware attacks, handouts and brochures containing guidelines and best practices will be disseminated to the healthcare organizations.

2 Cyber-attacks

Cyber-attack is an undesirable attempt to steal, disclose, modify, disable, or demolish data by illegal access to computer systems. Since these attacks involve the use of computers, such criminal activity is called cybercrime. The annual costs of cybercrime to the global economy are estimated to reach 5.5 trillion euros by the end of 2020, which is twice as high as in 2015 (European Commission, 2021). For example, in 2021, the average cost of data leakage due to cybercrime was US 4.24 million dollars worldwide and US 9.05 million dollars in the United States. These costs include detecting and responding to breaches, reducing working time and loss of income, and long-term reputation damage to businesses and their brands. Moreover, can lead to a loss of customer trust, fines from regulatory authorities, and even lawsuits (IBM, 2022).

2.1 Phishing attacks

Phishing is a semantic attack that uses the way people consider the content they read or hear to be important. In other words, semantic attacks, such as phishing, use the fact that people generally believe what they see and hear to force someone to take actions that they would not normally want to take (Heartfield et al., 2018). It is really difficult to develop purely technical approaches to prevent them because a semantic attack uses the way people assign meaning. Identifying and recognizing phishing messages is an important component of preventing phishing (Wash, 2020).

A message containing a hyperlink to a malicious website sent by a threat subject is commonly known as phishing when the threat subject attempts to obtain confidential information from a user who clicks on such a link. There is an example of a real phishing e-mail in Fig. 2 below.

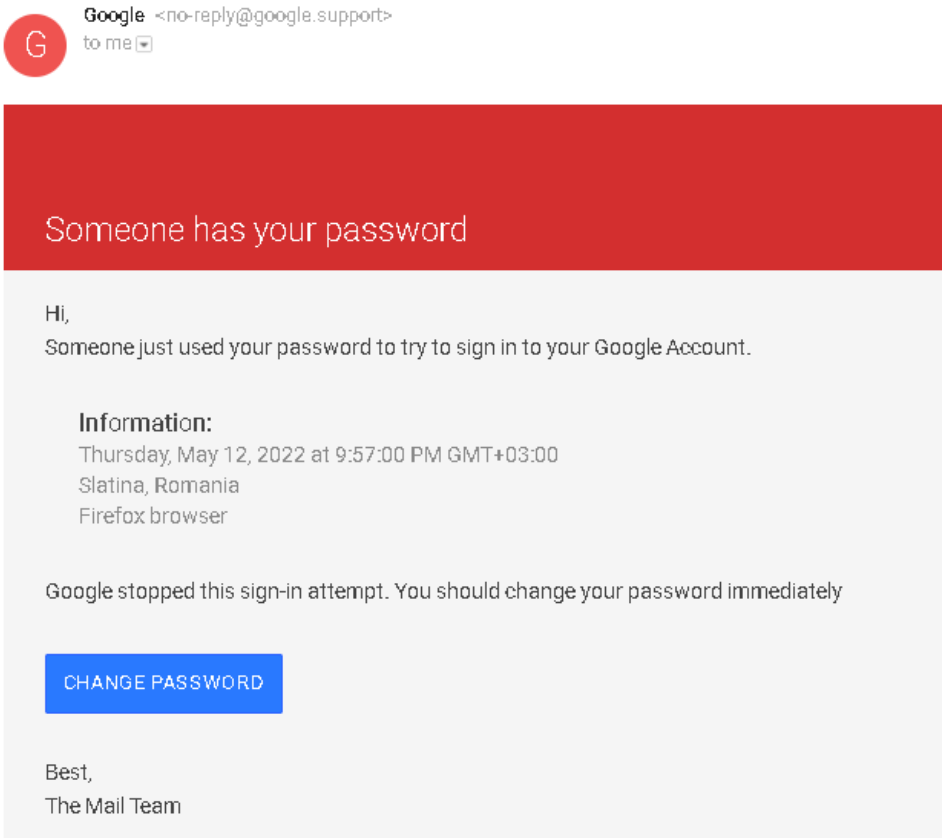

Figure 2. An example of a phishing attack.

Phishing attacks have become more frequent over the past few years. Phishing emails can be divided into two types: spear-phishing and business email phishing (Lam et al., 2019). Phishing attacks pose a particular problem when attackers target specific people or organizations, which is often referred to as “spear-phishing". People often fall for phishing attacks, and attackers are increasingly using persuasion methods to target individuals (Wash, 2020).

In phishing attacks on business emails, attackers imitate high-ranking employees’ email accounts and encourage targeted users to perform certain actions. The existing meaning of a phishing attack is variant and proposes diverse definitions, as can be shown in the table below. Lastdrager studied the definition of phishing and proposed the following agreed definition for the coordination of future research: “Phishing is a scalable deception activity, using imitation to obtain information from a target’’ (Lastdrager, 2014).

Table 1. Phishing definitions

Author	Definition
Chen et al.,2019	Phishing is a crime based on social engineering.
Sameen et al, 2020	A phishing attack is a fraudulent attempt to hide yourself as a trusted party to obtain sensitive information.
Chen et al., 2009	Phishing is a kind of online identity theft that combines social engineering and technical maneuvers

Phishing attacks are generally characterized by three aspects (Aleroud et al, 2017):

- The legitimate entity is forged.
- A website is used for spoofing.
- The data is requested and retrieved from confidential information.

The process of phishing attacks is presented in Fig. 3.

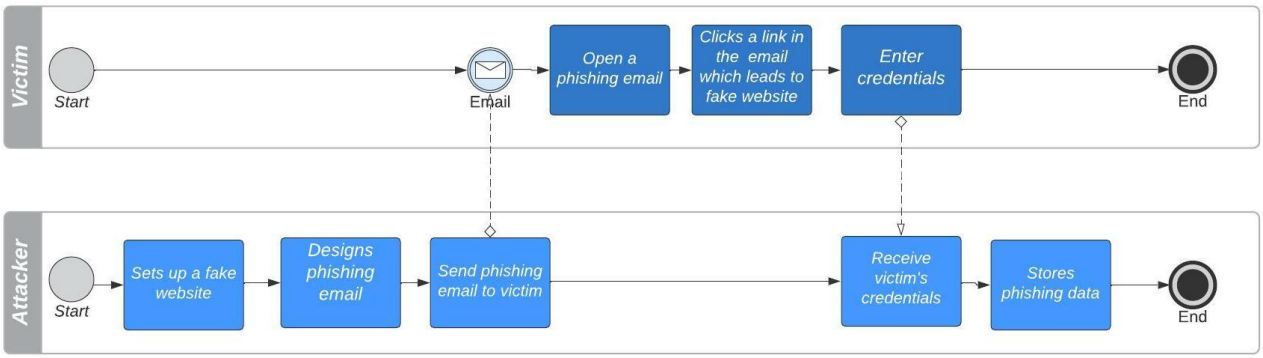

Figure 3. The process of a phishing attack (Adopted from (Jampen et al., 2020)).

Although most end-users are concerned about suspicious links, many end-users cannot distinguish between malicious websites that may cause data loss.

2.1.1 Recent cases of phishing attacks

Organizations often face phishing attacks, which are among the most serious threats to companies. According to Verizon's2021 Data Leak Investigation Report, 35 percent of all data leaks relate to fraud, which tries to steal personal or login credentials (Irwin, 2021).

Pyeongchang Olympic Games

A case of a spear-phishing campaign in January 2018 has been launched against companies participating in the Pyeongchang Olympic Games. The attackers used fake messages from real-looking email senders. The e-mail address belongs to the South Korean National Anti-Terrorist Centre, but it was sent from Singapore. The attackers tried to deceive the victims to open a malicious document containing malware in the form of a hypertext application file (Lam et al., 2019).

Google and Facebook

One hacker who posed as a computer parts salesman started a money-making scheme. It started with a spam email and resulted in a campaign the Business Email Compromise (BEC). For several years, companies have been paying bills that were forged by a fraudster in the amount of $ 100 million. For this, the cybercriminal received a sentence of imprisonment for a period of 5 years.

Sony Pictures

Sony Pictures film studio has been targeted by cybercriminals. A criminal hacker group called "Guardians of the World" in November 2014 reported a leak of 100 terabytes of data. Hackers found the necessary information about the names and positions of company employees on the LinkedIn website and posed as their colleagues. Hackers sent malicious emails containing malware to unsuspecting real employees (Computerworld, 2022).

As a result, company confidential information was stolen, including recently published files. In general, Sony lost about a hundred million dollars due to this phishing attack (Reuters, 2022).

FACC

In January 2016, due to a fake message from the CEO of the Austrian organization FACC, an employee fell for a phishing attack (Reuters, 2016). The employee received an email with a request to transfer more than 40 million euros to another account as part of the "purchase project". The message seemed genuine, but it was a scam. Since the employee could not determine that this email was phishing, he complied with the hacker's request and was

punished for it. FACC demanded damages in the amount of 10 million euros from the managers, but the Austrian court rejected the claim (Security News, 2022).

2.1.2 Recent cases of phishing attacks in the healthcare sector

One of the most efficacious phishing attack methods relies on employee vaccination surveys that appear to be sent out by Human Resources. For instance, approximately 65 percent of employees clicked on links in these fake emails and 48 percent put corporate credentials in false authentication forms in 2021(Positive technologies, 2022).

Several thousand Washington residents' sensitive medical records were exposed after successful phishing attacks by local public health agencies. The Spokane Regional Health District (SRHD) said the 1,260 people and two departments associated with "protected customer health files" could have been "previewed" by an attacker during the 24 February 2022 incident (The Daily Swig, 2022).

Kevin Mandia, CEO of FireEye, a cyber security company, provided some insight into the motives for the attack on these medical organizations. He told that more pharmaceutical companies, hospitals, health services, state-owned enterprises that do not have the ability and skills to protect themselves are being deceived. Maren Ellison, a chief information security specialist at Johnson & Johnson said that the organization faces more than 15 billion cybersecurity incidents every day (Mitchell, 2021).

2.2 Ransomware attacks

Ransomware is a sophisticated malware that uses strong encryption to exploit system weaknesses to host data and system functions. Cybercriminals use ransomware to ask for payments in exchange for system release. The recent development of ransomware is an addition to extortion tactics.

According to the data provided by the European Commission for Cyber Security, ransomware demand rose from 13 billion euros in 2019 to 62 billion euros in 2021. The

average ransom doubled from 71 thousand euros in 2019 to 150 thousand euros in 2020 (European Parliament, 2022).

According to the US Government's Office of Cyber Security and Infrastructure: "Ransomware is a form of ever-evolving malware that encrypts files on devices and makes the systems that depend on files and their usage unusable" (CISA, 2022).

Users can be exposed to this threat in a variety of ways. Ransomware can be downloaded to the system when involuntary users visit malicious or contaminated websites. It can also come in the form of a payload that is either deleted or loaded by other malware. Some attachments in spam emails consist of ransomware programs, which are downloaded from malicious pages through malicious advertising. The process of this attack is presented in Fig. 4 below.

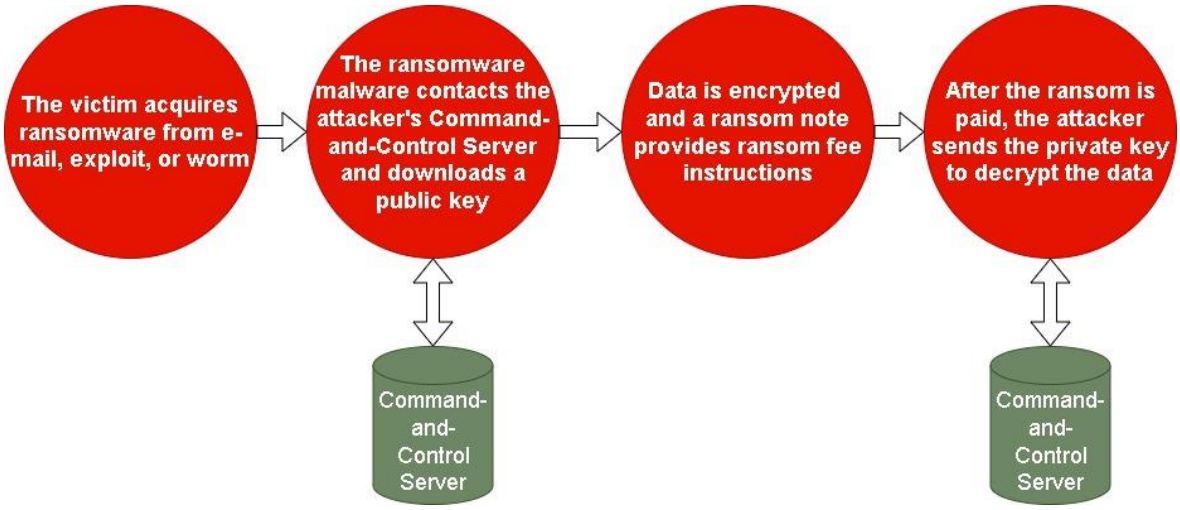

Figure 4. The process of a ransomware attack (Adopted from (ExtraHop, 2022).

Ransomware programs can lock the computer screen or encrypt pre-defined files in crypto ransomware. Two scenarios can be. In the first one, the person is prevented from using the computer because of the infection and the full-screen picture appears telling it. The picture on the screen is usually used for showing the information on how the victim can send the money for unlocking access to the computer. An example of this picture made by hackers is illustrated in Fig. 5.

Figure 5. An example of a ransomware attack (Digital Guardian, 2015).

The second way of a successful ransomware attack is when important or valuable files are encrypted and there is no way to save them expect paying the ransom fee to the hacker. If the victim rejects the payment, then all documents will be deleted. A ransomware program is regarded as «security software» because it forces users to pay fees (or ransomware) to scare them or intimidate them (Trend Micro, 2022).

2.2.1 Recent cases of ransomware attacks

Here are examples of the biggest ransomware attacks in the 2021 year.

Colonial pipeline case

Regarding all the cyber-attacks and attacks using ransomware in 2021, the violation of the Colonial Pipeline at the end of April received the most news coverage. As Joe Giordano, director of the cybersecurity program at Touro College in Illinois, notes, «The attack on the Colonial Gas Pipeline has had such an impact because the gas pipe is a critical national infrastructure system component.” The attack is particularly dangerous because consumers are panicking and neglecting precautions.

The attack, which hit many consumers near home, is due to the direct effects of the oil shortage on most Americans. Through a virtual private network (VPN) cyber attackers penetrated the company's networks and disrupted the operation of the pipeline. DarkSide had blocked the pipeline that transports 45% of the gas and jet fuel supplied to the part of the United States (Security Intelligence, 2021). The Darkside hacker group was behind the attack, focusing on company billing systems and internal business networks, leading to a wide shortage in many states. Fortunately, the U.S. government has recovered most of the $4.4 billion ransom. The FBI tracks the cryptocurrency and digital wallets and tracks money (The New York Times, 2021).

Brenntag case

At the beginning of May 2021, DarkSide attacked a Chemical Distribution Company Brenntag. Darkside demanded $7.5 billion in bitcoin after they stole 150GB of data. Brenntag quickly abandoned the demand and finally paid $4.4 million. It reached only half the initial demand but remains one of the highest ransomware payments in history (Irwin, 2021).

AXA and CNA insurance companies' cases

In May 2021, the European AXA insurance company was attacked. Shortly after the company announced significant changes to its insurance policies, the incident occurred. AXA said it would stop reimbursing many customers for payment of ransomware. The unique attack on the cyber insurance company caused headlines and hackers accessed 3TB of data (Security Magazine, 2021).

In March 2021, another major insurance company was attacked by ransomware. On March 21, the CNA network was attacked by hackers and 15000 devices were encrypted, including many remote workers' computers.

Kaseya case

Although the name Kaseya is not widely known to consumers, it manages the IT infrastructure of large companies around the world. Like the attacks on Colonial Pipeline

and JBS Foods, this hack could potentially cause serious damage to key areas of the economy (Touro College Illinois, 2021).

REvil penetrated Kaseya's direct and client customers because the hacker group sent fake software updates via Kaseya's virtual system administrator. According to Kayesa, about 50 of their customers and a total of about 1,000 businesses were affected. The hacking group asked for $70 billion in bitcoins. As a result of the cyberattack, Swedish supermarket chain Coop closed 800 stores for a week (BBC News, 2022).

2.2.2 Recent cases of ransomware attacks in the healthcare sector

In times of crisis, many hackers use chaos and agitation to seek potential financial gains. With the arrival of the 2020 pandemic, cyberattacks in the health sector have been drawing greater attention. A Comparitech study (2020) showed that ransomware attacks had a significant financial impact on the medical sector. In 2020, more than 20 billion dollars were lost due to declining revenues, lawsuits, and ransom payments. Over 600 hospitals, clinics, and other medical facilities were subjected to 92 successful ransomware attacks.

As the pandemic continues to have a major impact on all organizations, corporate newsletters with coronavirus themes are still common. The attackers often disguise the email as a work email and this method is often successful.

In the recent years, a destructive ransomware program attacked the Finnish mental health startup Vastaamo. Personal information of patients and the details of their meetings have been stolen, and hackers threaten to leak these data if individuals do not pay the ransom (AskCyberSecurity, 2022).

However, not only the finances of patients and data are at risk, as ransomware attacks are critical to health care and can also cause deaths. According to NBC News, Tyranny Kidd filed a lawsuit against the Spring Hill Medical Center in Alabama for failing at birth (NBC News, 2021). In 2019, the hospital suffered ransomware attacks that closed its IT infrastructure. The hospital did not inform a woman of the attack. Kidd and her child did not attend key tests that prevented her from being seriously injured in the head nine months after

her death. This is just one example, and it is likely to see more terrible forms of cyber-attacks that threaten human lives.

2.3 Impact and threats of cybersecurity attacks

What impact do cyber-attacks have?

Cyber-attacks can destroy businesses if they were carried out successfully. They can cause significant downtime, data loss, data manipulation, and ransom money losses. During downtime, a service failure or financial loss can occur. In addition, cybersecurity threats lead not only to monetary losses but also to human casualties.

How often phishing attacks were carried out in 2021?

Phishing attacks account for more than 80 percent of the reported security incidents. According to CISCO's 2021 Cyber Security Threat Report, about 90 percent of data leakage is caused by phishing. According to a 2021 ESET survey, between May and August 2021, email attacks increased by 7.3% (Spanning, 2021).

In 2021, how many ransomware attacks have been committed?

In September 2021, SonicWall reported about 500 million attacks and 1,748 attempts to attack organizations (Jr, 2021). This is equivalent to companies facing 9.7 extortion attempts a day. The firm's report on cyber threats for 2021 also notes the global attack using ransomware grew by a staggering 48 percent, while the UK increased by 233 percent and the US grew by 127 percent. According to the Blackfog report on the state of ransomware for 2021, cybercriminals' main targets are government agencies, education, health care, services, technology, manufacturing, and retail (Spanning, 2021).

What percentage of ransomware is phishing?

Above than 90 percent of cyber-attacks penetrate organizations via email. According to the FBI, phishing attacks have increased by 400% year-on-year. In 2020, cyberattacks and ransom payments increased. According to the Harvard Business Review, organizations paid cybercriminals 300% more. The sudden increase in remote work and the weakness of domestic security have given hackers a great opportunity to destroy sensitive data (Sharton, 2021).

3 Methodology

This section aims to describe the thesis methodology. The methodology consists of two main parts, which are conducting a systematic literature review and explaining the idea and methods of conducting a co-design workshop.

3.1 Literature review

To carry out this thesis, a systematic review of the literature was the main method of research. A systematic review of existing literature seeks to solve this problem by looking for relevant qualitative papers on certain research issues. This requires a systematic search process to solve specific research questions, that were created for this SLR and which are listed below:

1. What are the mitigation strategies against phishing attacks?
    i. How can they be classified? (best practices, guidelines, tools)
2. What are the most focused phishing vectors in the development of mitigation strategies?
3. What are the open issues which emerge from existing literature?

To classify and acknowledge the landscape of existing phishing interferences, a systematic review of the literature was conducted, following the guide "preferred reporting elements for systematic review and meta-analysis" (PRISMA). It is argued that literature reviews take a necessary part in the development of information about the subject area, for example, by summarizing previous research papers, identifying research gaps, and developing a research program (Das et al, 2020).

The literature review has five phases. (i)The first phase helped to identify the existing literature through the search that was done in the search line. (ii) Due to the huge number of sources that the automatic search produced, it was decided to apply a time filter to reduce the number of sources. (iii)After this, the duplicates were removed, and papers were screened by their title and abstract. (iv) During the screening phase, most papers were excluded due

to a lack of necessary information for further analysis. (v) The next stage was checking the eligibility of the articles. Some of them were excluded because of the closed access, so for reading them the money must be paid. Few studies were eliminated due to not meeting the inclusion and exclusion criteria. The whole process of choosing an article is illustrated in Fig 6 below.

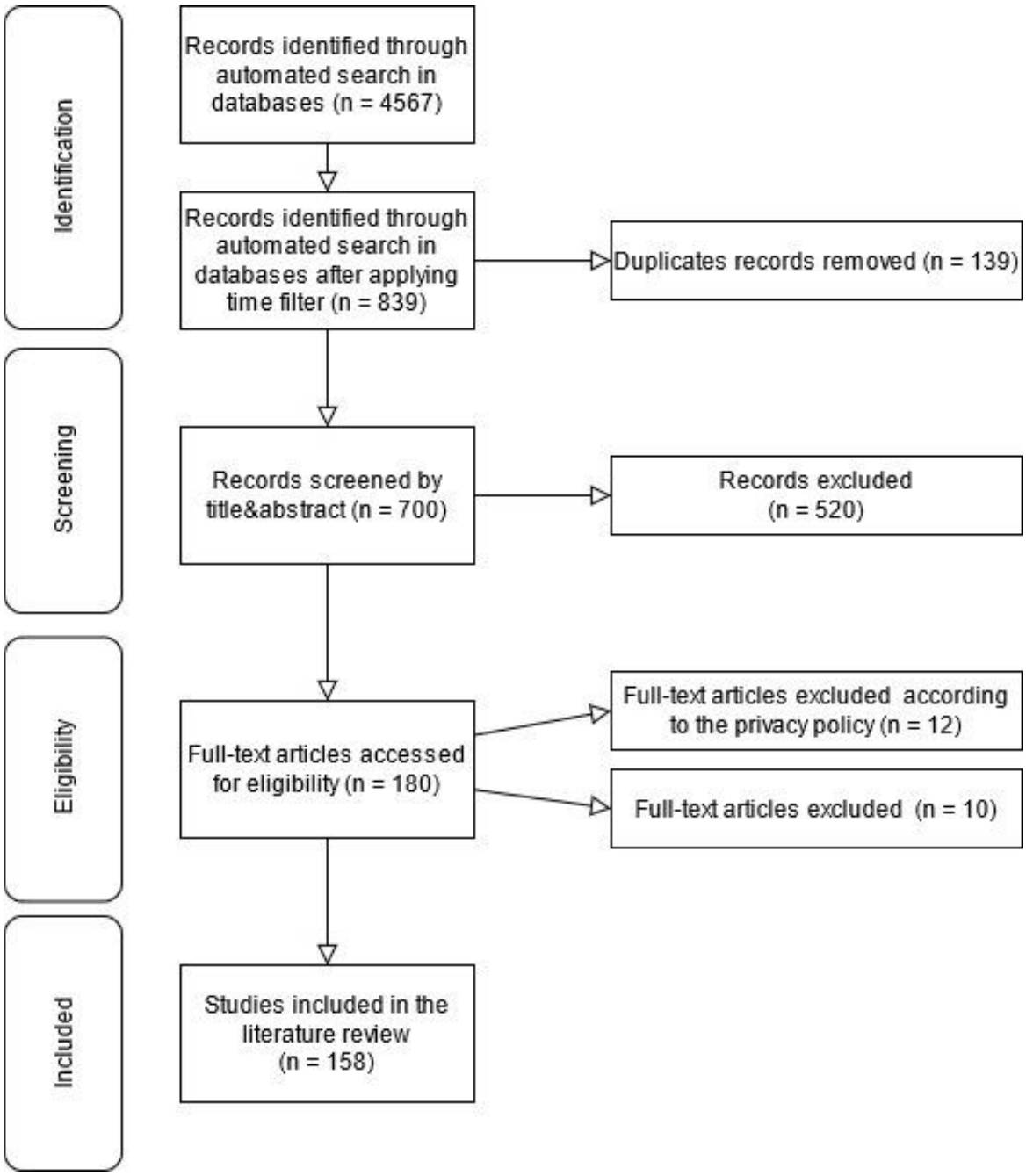

Figure 6. The process of systematic literature review.

3.1.1 Search string

Based on the research questions final keywords were defined for the development of future search queries. Then the data source (i.e. most relevant data identifying research tasks and evaluating are phishing, guidelines, best practices, tools, prevention techniques, prevention, mitigation, and solutions.

The query below was used to take all the relevant papers from different databases: “Phishing” AND “guidelines OR best practices OR tools OR prevention techniques OR prevention OR mitigation OR solutions”.

In addition, the following query was tried: (Phishing AND (guidelines OR best practices OR tools OR prevention techniques OR prevention OR mitigation OR solutions)) to see if there is a difference between separate requests and the one long request.

3.1.2 Databases for executing the search

In the thesis, search strings were executed in several databases to retrieve related documents and articles. On the list below there are selected databases.

1. Springer
2. IEEE
3. Web of Science
4. ACM
5. Scopus (Elsevier)

The following results were found after the first string search and are represented in the table below.

Table 2. Articles in databases

Databases	All results from queries
ACM	381
Scopus	274
IEEE	567

Web of Science	1100
Springer	2245
Total	4567

As it takes a long time to read all the available papers from databases it was necessary to shorten the time to get more relevant and recent resources. A search was performed in the range of years from the beginning of 2019 to March 2022. Results are represented in the table.

Table 3. Articles in databases after applying a time filter

Databases	Results after applying a time filter
ACM	84
Scopus	48
IEEE	233
Web of Science	304
Springer	170
Total	839

3.1.3 Selection of the papers

In line with the SLR guidelines, it is essential to remove all the repeated resources that might be in different databases. The process of resource selection on the third phrase, which is named ‘Remove duplicates’ had the logic illustrated in Fig 7.

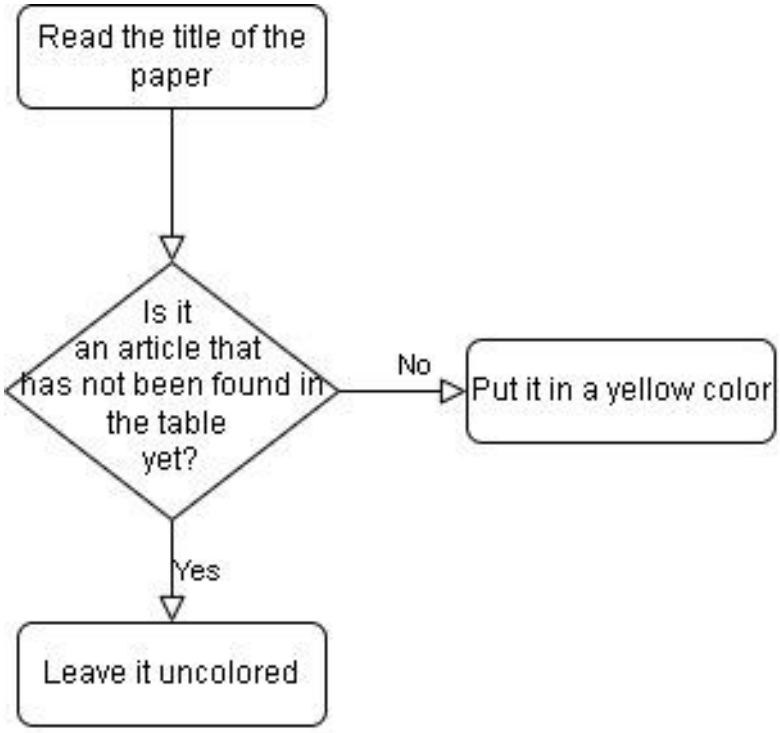

Figure 7. The process of resource selection on the third phrase.

The following table presents the results of this stage:

Table 4. Articles in databases after applying selection on the third phase.

Databases	All results	Duplicates (in «yellow»)	«Uncolored» results for future consideration
ACM	84	11	73
Scopus	48	3	45
IEEE	233	11	222
Web of Science	304	111	193
Springer	170	3	167
Total	839	139	700

The criteria for inclusion and exclusion assist to select applicable research documents based on research questions. This works as a standard that must be maintained for every article. The criteria of inclusion and exclusion that have been followed in the review of this literature are as follows. These were applied to all papers obtained from different databases.

Table 5. Criteria for inclusion and exclusion

Inclusion criteria	- The publication reports at least one mitigation strategy against phishing attacks. - The language of publication is English. - In case the strategy is reported in more than 1 publication, the most recent one will be retained.
Exclusion criteria	- Articles with missing abstracts/notes. - Partly available.

Decision-making at this stage is illustrated in figure 8 below.

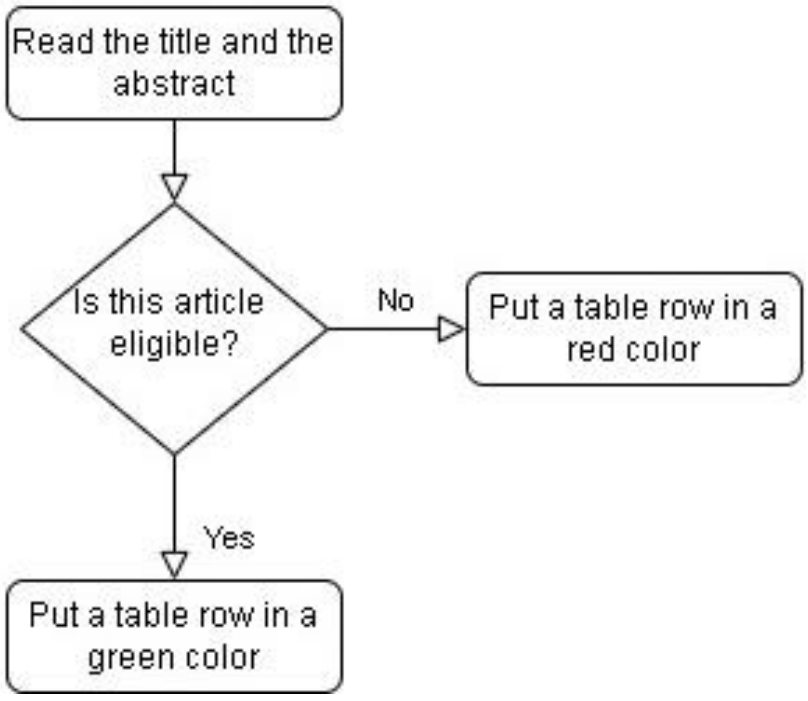

Figure 8. The process of decision-making

Table 6. Articles in databases after screening

Databases	All results without duplicates	«Red» results	«Green» results for future consideration
ACM	73	47	26
Scopus	45	29	16
IEEE	222	163	59
Web of Science	193	128	65

Springer	167	153	14
Total	700	520	180

After fulfilling the inclusion-exclusion criteria and selecting studies, there 180 articles were selected for full-text scanning. Therefore, during the last stage, 180 articles were fully read; however, not all of them met all inclusion criteria during the full-read. The number of articles was excluded due to the privacy policy because it was necessary to buy the full access to read them. In the result, it was concluded with 158 articles from all databases for further consideration.

3.1.4 Extraction and synthesis of the data

The extraction of data from systematic literature reviews helps to determine what information to collect from articles to identify research tasks. The whole data extracted from articles are saved to an Excel file for further analysis. The screenshot is presented below.

Name of the publication	Name of the solution proposed	Classification	Solution Proposed	Targetted Phishing vector (email, eFax, Instant Messaging, SMS, Social Network, Vishing (phone calls, voice messages), Website, WiFi)	Underlying methodology of the solution (Machine Learning, Cryptography, Hardware etc.)
Finding Phish in a Haystack: A Pipeline for Phishin	CTL Detection Pipeline	Approach	One possible approach is to detect phishing	Website	Machine Learning
A Framework to Protect Against Phishing Attacks	-	Framework	The proposed framework has two major	Generic	Gamification
A Phishing Mitigation Solution Using Human Behav	-	Approach	The solution assigns proper	Generic	Machine Learning
Following Passive DNS Traces to Detect Stealthy M	-	Scheme	We design novel	Website	Machine Learning
Human Risk Factors in Cybersecurity	-	Recomendations	After some experiments our	E-mail	Knowledge transfer
A Comparison of Natural Language Processing and	-	Method	This research focused on the comparison of	Generic	Machine Learning
Click This, Not That: Extending Web Authentication	-	System	We presented two techniques – web tripwires	E-mail	Hardware
PhAttApp: A Phishing Attack Detection Application	PhAttApp	Solution	A phishing detector application,	E-mail	Knowledge transfer
Secure Email Login Based on Lightweight Asymmetr	-	Solution	a secure login scheme based on	E-mail	Cryptography
A Flexible Phishing Detection Approach Based on S	-	Approach	a new scalable phishing detection approach	Website	Programming
Detecting Telephone-Based Social Engineering Atta	ntiSocial Engineering Tool (ASsET	Approach	A social	Vishing	Machine Learning
How Experts Detect Phishing Scam Emails	-	Recomendations	It would be helpful if phishing training could	E-mail	Knowledge transfer
Detecting Spam Tweets Using Machine Learning an	-	Approach	we propose an	Social Network	Machine Learning
Augmenting Phishing Squatting Detection with GAN	-	Solution	We propose the	Website	Machine Learning
Visualizing and Interpreting RNN Models in URL-Ba	-	Model	we took the deep learning approach and built	Website	Neural network
Avoid Phishing Traps	-	Recomendations	We have used annual phishing quizzes with	Generic	Knowledge transfer
A Design of an Anti-Phishing Training System Colla	-	System	An education system that	E-mail	Hardware
LinkMan: Hyperlink-Driven Misbehavior Det	LinkMan	Approach	LinkMan can categorize these hyperlinks as: a)	Social Network	Machine Learning
URL-Based Phishing Detection Using the Entropy of	-	Framework	a new feature called the entropy of NAN	Website	NonAlphanumeric
What.Hack: Engaging Anti-Phishing Training Throu	What.Hack	Framework	the game What.Hack, which not only teaches	E-mail	Gamification

Figure 9. Screenshot from Excel file

The name of the column that was created for collecting the necessary data is given below:

1. Name of the publication.
2. Name of the solution proposed.
3. Classification.
4. Solution proposed.
5. Targeted Phishing vector (email, eFax, Instant Messaging, SMS, Social Network, Vishing (phone calls, voice messages), Website, WiFi).

6. The underlying methodology of the solution (Machine Learning, Cryptography, Hardware, etc.).
7. Target area (general, banks, healthcare, users, etc).
8. The main feature of the solution.

To synthesize the data extracted, the focus was on the point that the article must contain guidelines and recommendations for preventing phishing attacks. The dataset was analyzed by searching for papers that presented some solutions. The results of the SLR are presented in section 4. Further, these existing solutions and guidelines that were collected will be represented by groups and visually in the thesis. Therefore, new knowledge will be developed to present in the co-design workshop.

3.2 Participatory Research

Participatory research (PR) is an approach from research to action that emphasizes the direct involvement of local priorities and perspectives (Comwall et al., 1995). The basic presumption of PR methods is the value of human participation itself. It includes methods that make it possible to speak out, participate, test yourself, and be perceived as a person who has the right to self-expression and is appreciated by others (Abma et al., 2019). This type of research has its frameworks and approaches and one of them is user-centered design.

User-centered design method, which began in the 1970s and spread in the 1990s, was the most useful to design and develop consumer products (Sanders, 1992). User-centered design is an iterative design process involving users in the development of products or services that are ultimately intended for them. (Vaughn et al., 2020). However, user-centered design approaches are now emerging as not able to address the scope and complexity of today's challenges.

The user-centred design approach (user as subject) is primarily a phenomenon driven by the United States. Since the year 1970, people were given some possibility for an initiative in providing expertise and taking a part in the generating activities at the beginning of design phases. People in Northern Europe lead a participatory design (users as partners). Both approaches are beginning to affect each other.

The map below shows the different approaches presented along the two axes: the user role (horizontal) and the research approach (vertical).

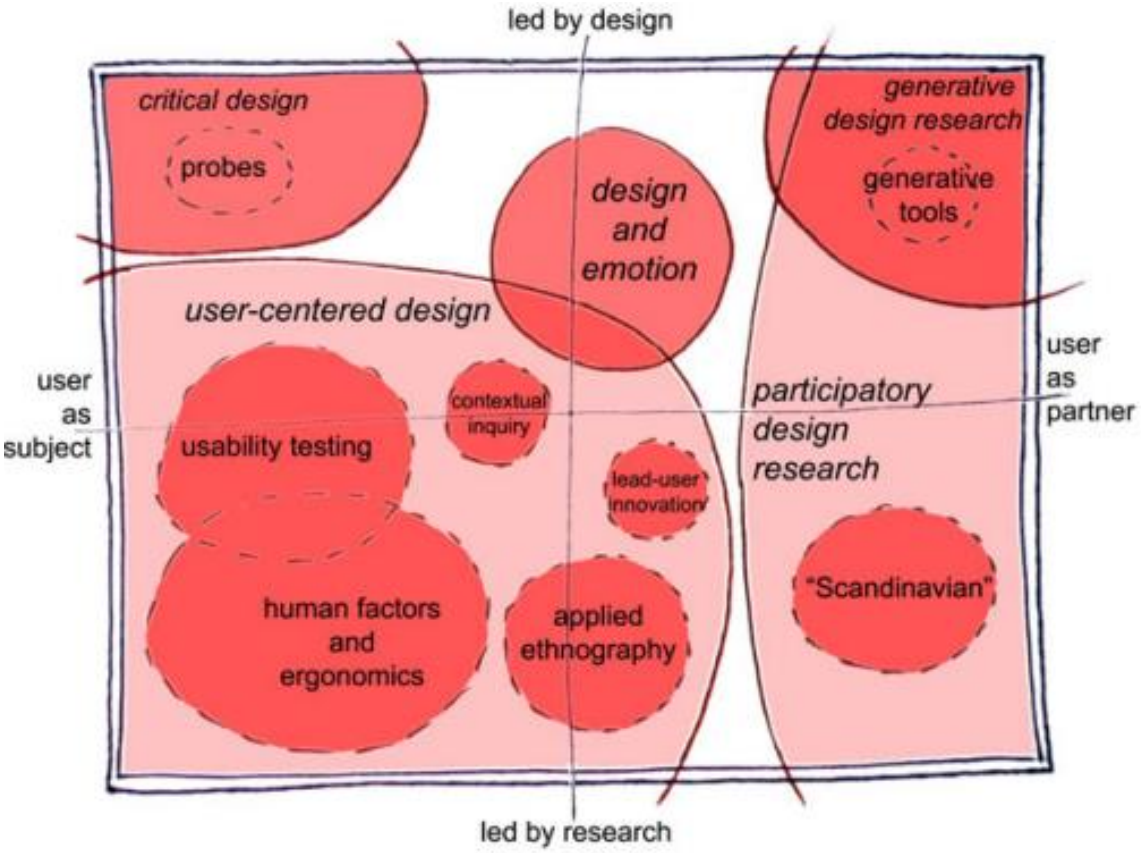

Figure 10. The map of design research (Sanders et al., 2008).

Participatory design (PD) is a rapidly growing field (Sanders et al., 2010). Participatory Design is a design practice in which various non-designers participate in various collaborative design activities during the design process. The participatory design process usually involves people with different backgrounds, interests, and roles in the project. Therefore, an important task is to find suitable ways to involve and involve people in traffic regulations (Sanders et al., 2010).

A recent study suggests that designers collaborate with others to create innovative concepts and ideas, rather than creating themselves. Transformation design is the latest field of emerging design and is based on a combination of participatory practices and user-focused methods. To solve social and economic problems using traditional design skills, it uses design processes as a means of enabling cooperation between diverse disciplines and

stakeholders. New design practices focus on people's or social needs and require different approaches because they must develop longer views and address broader fields of investigation.

Definition of the co-design approach

Co-design is an act of creation in the design process. In particular, with stakeholders, the results are vetted and used to meet their needs (Medium, 2022).

Based on participatory design and user-focused design, the aim is to involve stakeholders at the stages when the design process only has started. Participation levels vary from information on projects to «users as partners» in design, and everyone can become creative (Sanders et al., 2008). Instead of focusing on 'designing for people', it focuses on 'designing for people'. It is an instrument to discover and explore opportunities, not to make final decisions, to start discussions between stakeholders, and guiding design decisions. For example, create a concept that communicates what designers should design and who should design it. Usually, design specialists facilitate joint design seminars by guiding participants through the design process and using their experience in this topic (Medium, 2022).

The collaborative design method has been divided into four phases (Sanders et al., 2014). The first phase is called pre-design, the second is called the generative phase, the next is the evaluative phase, and the last one is the post-design phase. The design phases can be compared between each other as it is shown below.

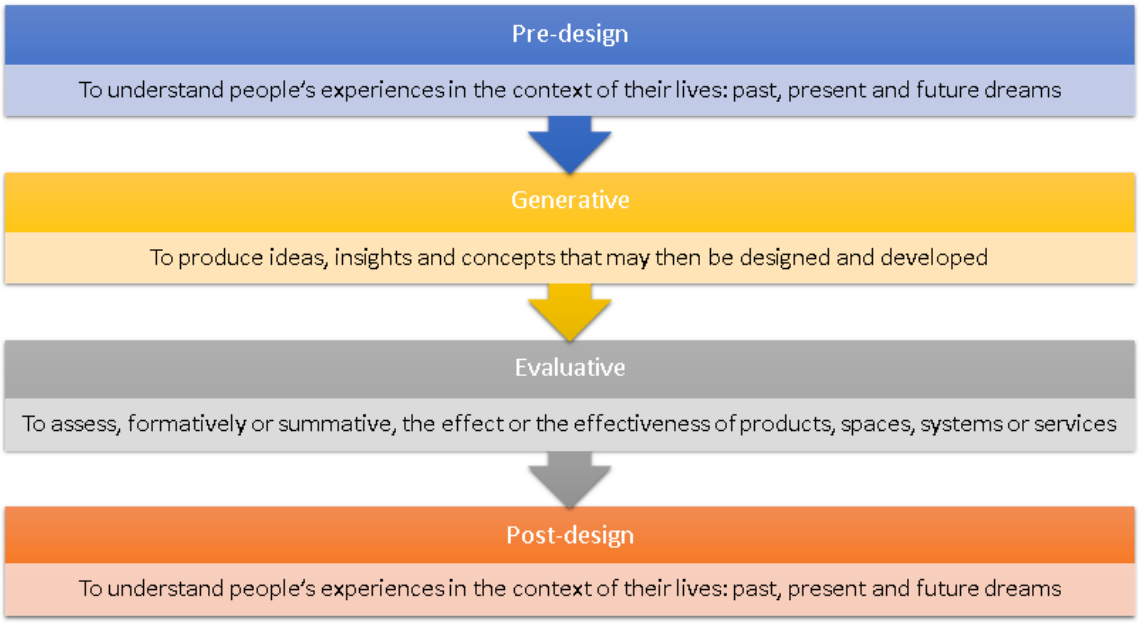

Figure 11. The design phases (Sanders et al., 2008).

Co-design plays a mixed role: those who ultimately participate in the design process play a significant role in the development of knowledge, the creation of ideas, and the development of concepts. Through the generation of ideas, researchers provide tools to create ideas and expressions. Designers and researchers collaborate on tools to create ideas, design skills are essential for tool development. However, the designer and the researcher might be the one person.

The solution to the persuasion and blind spot problem is participation. The collaborative design workshop fully meets this need and improves the product design process unexpectedly in two ways: speed and quality. A well-organized workshop can generate a wide range of ideas that go beyond what one person can create (Sanders et al., 2008).

The methods for conducting a co-design

Examples of research methods used at collaborative design meetings include various ideas (UX Magazine, 2012). The materials used at every workshop must be tailored to meet the research requirements and must vary according to the research.

Table 7. Methods of co-design approach ideas (UX Magazine, 2012)

Methods	Description
Collages	Mostly collages are used to identify emotions or desires. People can use collages to show themselves through images and words that can visualize how a person imagines his current or future. The selected pictures and words should be abstract to evoke a dialog excluding directing the attendees in some way.
Mapping	Mapping is the process of creating mental maps of abstract concepts, events, procedures, or systems. For example, arrows, and regular and irregular shapes are used as symbolic elements. In addition, some distinctive icons or words can be also used for helping the attendees of the co-design workshop to express the flow of a process.
Storyboards	Storyboards are good tools for collaboration and are used to describe the events and steps of the journey. Some storyboard materials include drawing materials that help participants without being prescribed. The participants receive some pre-defined elements with a storyboard based on the project stages and research questions. For instance, designers may have already shown some steps, but participants must add dialogues and text explanations.
Cards	Future scenarios and characters can be developed together using the inspiration card as a story. These cards can be manufactured by design and research teams. Cards contain many images, words, or complete sentences. Participants use cards to create stories and place them on large walls in their preferred order.
Modeling	Modeling consists of, for example, physical mockups of material products, or travel experiences. For jointly designing group dynamics or deconstructing complex systems modeling can also be used. Modeling tools include some 3D figures

	made of many different materials or constructors (LEGO, Mecano, etc.).
Diaries	Diary research provides self-reports and longitudinal records of user behaviors and attitudes, which researchers later analyze and analyze to better understand habits and behavior patterns. Study participants may be asked to record data as events occur or at specific time intervals (for example, via email or text message at certain times of the day).
Games	For collaborative design, such methods as brainstorming, design, and innovative games can all be applied differently. An idea for doing it for people can be found in books. For example, in the book “Innovative Games" by Luke Homan.

According to the study conducted by Sanders (2010), it can be illustrated that different methods can be compared by context.

Table 8. Applications of the methods of Participatory Design are described by the context

	Collages	Mapping	Storyboards	Postcards	Modeling	Diaries	Games
Individual	+	+	+	+	+	+	+
Group	+	+	+	+	+	-	+
Face-to-face	+	+	+	+	+	+	+
Online	+	-	+	-	-	+	-

This comparison shows that most of the methods can be used individually and in groups.

4 Results

This section reports the findings of the systematic literature review and presents the proposal for a co-design workshop.

4.1 Findings from the literature review

At the beginning of this subsection, the answers to the three research questions created especially for the SLR will be discussed. The first question of the literature review is below: **What are the mitigation strategies against phishing attacks? How can they be classified?**

As an answer to the first SLR research question, the classification was created that considered the following terms based on the synthesis of the data:

- A *system* is a tested system that consists of several modules.
- *Models & methods* is a created term that consists of a combination of models and methods that can be used against cyber-attacks.
- *Guidelines & recommendations* is a created term that is used to identify a combination of existing guidelines and recommendations.
- A *framework* is an additional part of the implementation of systems.
- An *approach* is a whole way with which the cyber-attack is to be prevented. Mostly included different processes combined into one approach. For example, conducting a training session and quizzes.
- A *tool* is a program that can help in the prevention of cyber-attacks. For example, a browser extension.

After conducting the systematic literature review, the following results were identified. The table below can provide an idea of what is the prevention mechanism against phishing attacks.

Table 9. The statistics of prevention mechanisms with references

Mitigation mechanism	Number of articles	References
System	29	(Valentim et al., 2021), (Lam and Kettani, 2019), (Barron, So and Nikiforakis, 2021), (Rao and Pais, 2019), (Mishra and Soni, 2021), (Adebowale, Lwin and Hossain, 2020), (Niroshan Atimorathanna et al., 2020), (Martins de Souza et al., 2020), (Sameen, Han and Hwang, 2020), (Lin et al., no date), (Fouss et al., 2019), (Nik Aein Koupaei and Nazarov, 2020), (Adebowale and Lwin, 2019), (Liu et al., 2019), (Yang and Su, 2019), (Higashino, 2019), (Lambat et al., 2021), (Al-hamar and Kolivand, 2020), (Cho, Bartlett and Freedman, 2021), (Higashino et al., 2019), (Megha, Raman and Sherly, 2019), (M, Janet and Reddy, 2020), (Halgaš, Agrafiotis and Nurse, 2020), (Sreenidhi et al., 2022), (Helmi et al., 2019), (Al-Hamar et al., 2021), (Bozkir and Aydos, 2020), (Li, Zhang and Guo, 2021), (Haney and Elaarag, 2021)
Models & methods	39	(Vaishnavi et al., 2021), (Ortiz Garcés, Cazares and Andrade, 2019), (Almeida and Westphall, 2020), (Ndagi and Alhassan, 2019), (Ishikawa et al., 2020), (Xuan, Dinh and Victor, 2020), (Roopak, Vijayaraghavan and Thomas, 2019), (Sonowal, 2020b), (Listík et al., 2019), (Arduin, de Oliveira and Kolski, 2021), (Le Page and Jourdan, 2019), (Tchakounte et al., 2018), (Ozcan et al., 2021), (Sornsuwit and Jaiyen, 2019), (Liew et al., 2019), (Sonowal, 2020a), (Luh et al., 2020), (Mridha et al., 2021), (Alsariera, Elijah and Balogun, 2020), (Bountakas, Koutroumpouchos and Xenakis, 2021), (Alkawaz et al., 2021), (Subairu et al., 2020), (Alhamad, Alzyadh and Badawi, 2020), (Shukla and Sharma, 2020), (Fetooh, El-Gayar and Aboelfetouh, 2021), (Page et al., 2019), (Kumar et al., 2020), (Singh and Meenu, 2020), (Wahsheh and Al-Zahrani, 2021), (Sonowal,

		2021), (Kumar and Sinha, 2021), (Aljofey et al., 2020), (Naaz, 2021), (Burda, Allodi and Zannone, 2020), (Al-Fayoumi, Alwidian and Abusaif, 2019), (Abdulhamid, Gana and Shafi, 2020), (Cui et al., 2021), (Balogun et al., 2021), (Feng and Yue, 2020)
Guidelines & recommendations	21	(Althobaiti, Jenkins and Vaniea, 2021), (Sadiq et al., 2021), (Gomes, Reis and Alturas, 2020), (Venkatesha, Reddy and Chandavarkar, 2021), (Manyumwa et al., 2020), (Moul, 2019), (Argaw et al., 2020), (Jampen et al., 2020) ,(Wash, 2020), (Cuchta et al., 2019), (Abroshan et al., 2021b), (Priestman et al., 2019), (Beaman et al., 2021), (Gomes, Reis and Alturas, 2020), (Argaw et al., 2019), (Dam and Deshpande, 2021), (Lim, Zhou and Zhang, 2021), (Desolda et al., 2019), (Tandale and Pawar, 2020), (Manjezi and Botha, 2018), (Adil et al., 2020)
Frameworks	16	(Ramluckan, van Niekerk and Martins, 2020), (Lee, 2020), (Kasim, 2021), (Maurya, Singh and Jain, 2019), (De La Torre Parra et al., 2020), (Alotaibi, Al-Turaiki and Alakeel, 2020), (Alsariera, Elijah and Balogun, 2020), (Bhardwaj et al., 2021), (Aung and Yamana, 2019), (Tang and Mahmoud, 2021), (A Younis and Musbah, 2020), (S. and Ravi, 2020), (Cernica and Popescu, 2020), (Mukhopadhyay and Prajwal, 2021), (Wen et al., 2019)
Approaches	42	(Jain and Gupta, 2019), (Azeez et al., 2021), (Chen and Chen, 2019), (Nirmal, Janet and Kumar, 2021), (Priya, Selvakumar and Velusamy, 2020), (Baillon et al., 2019), (Butt et al., 2021), (Shahriar et al., 2019), (Bhoj et al., 2021), (Paliath, Qbeitah and Aldwairi, 2020), (Bathala et al., 2021), (E and A, 2019), (Islam et al., 2021), (Miao and Wu, 2020), (Alzamil et al., 2020), (Wang and Duncan, 2019), (Abroshan et al., 2021a), (Nishikawa et al., 2020), (Wu et al., 2019), (Steverson et al., 2021), (Daengsi, Pornpongtechavanich and Wuttidittachotti, 2021), (Korkmaz et

		al., 2021), (Ariyadasa, Fernando and Fernando, 2020), (Kardaş et al., 2021), (Derakhshan, Harris and Behzadi, 2021), (Silveira et al., 2021), (Korkmaz, Sahingoz and Diri, 2020), (Drichel et al., 2021), (Awasthi and Goel, 2021), (Guo et al., 2021), (Abbas et al., 2021), (Stoleru, Popescu and Gavrilut, 2018), (Taha, 2021), (Mao et al., 2019), (Yongjie Huang et al., 2019), (Shaik et al., 2021), (Zhou et al., 2020), (Athulya and Praveen, 2020), (Nabeel et al., 2020), (Adebowale et al., 2018), (Bikov et al., 2019), (Dukarm, Dill and Reith, 2019)
Tools	11	(Steves, Greene and Theofanos, 2020), (Hr et al., 2020), (Boukari, Ravi and Msahli, 2021), (Zhu, 2020), (Ismail, Alkawaz and Kumar, 2021), (Brites and Wei, 2019), (Khan et al., 2021), (Datta et al., 2021), (Nathezhtha, Sangeetha and Vaidehi, 2019), (Yuankun Huang et al., 2019), (Ulqinaku, Lain and Capkun, 2019)

As shown in the table, most articles presented approaches. In the second place, the models & methods were presented. The least number of solutions from the articles was classified as a tool.

The existing solutions can be classified into these categories:

1. Cryptography.
2. Data mining.
3. Human-centric.
4. Fuzzy logic.
5. Machine learning (Including Neural networks).
6. Blockchain.
7. Pseudonymisation technic.
8. Hardware.
9. Programming.

The classification of mitigation strategies from the SLR has been done visually and has shown below in figure 12.

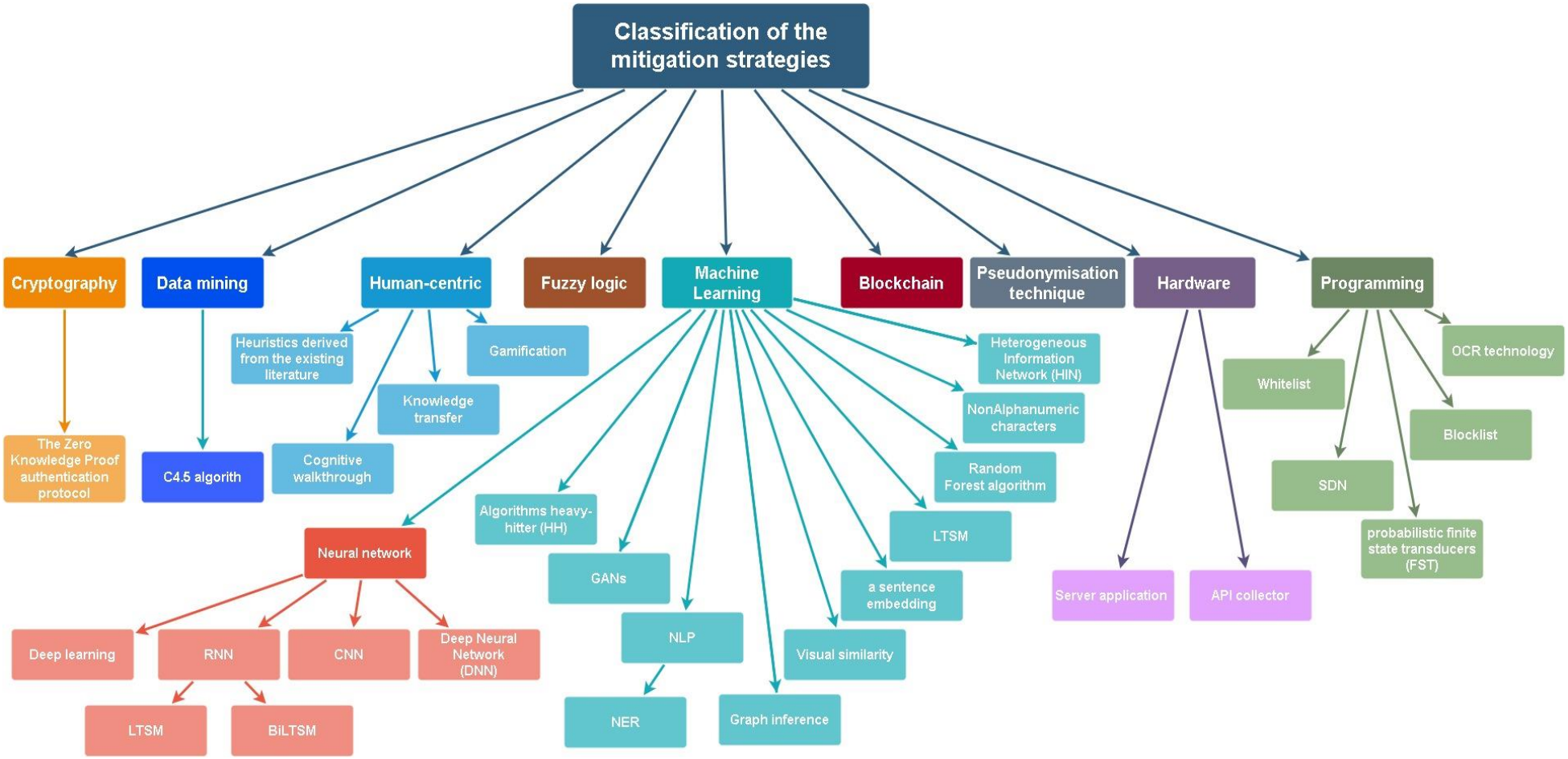

Figure 12. Mitigation strategies from SLR.

What are the most focused phishing vectors in the development of mitigation strategies?

To answer the second SLR research question the classification for the phishing vectors was implemented. The categories of phishing vectors were taken from the different studies.

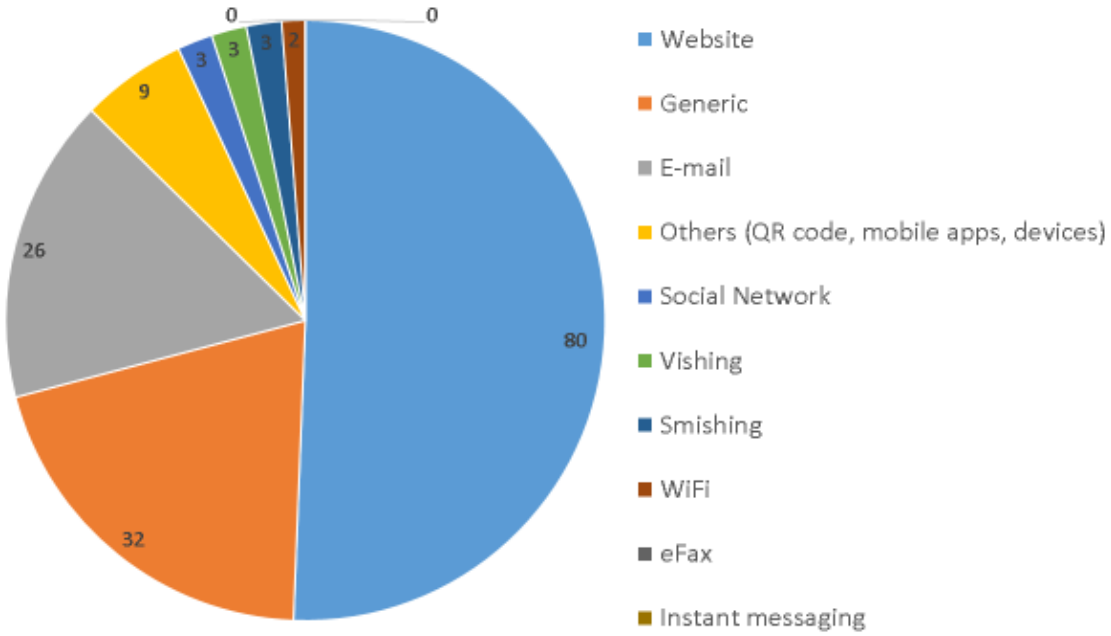

Figure 13. Phishing vectors from SLR.

According to the picture, the most focused phishing vector is websites as it takes more than a half of analyzed articles (80 papers). In the second place, the generic vector is located. In the third position, the e-mail vector takes place (in total, 26 papers). Further, nine papers were explaining the idea of preventing cyber-attacks on QR codes, mobile apps, and devices. It was grouped in the vector named “Others”.

Unfortunately, there were no results for eFax instant and messaging from the literature review. Therefore, more solutions related to preventing cyber-attacks through instant messaging can decrease the quantity of cybercrime.

What are the open issues, which emerge from existing literature?

Risk-taking behavior is an issue for phishing prevention

Through conducting a systematic literature review, it was found that an overall risk-taking level might grow the likelihood of opening a phishing e-mail. In addition, women appear to be more likely to click on a phishing e-mail. However, it must be indicated that these results may vary in different cultures and countries (Abroshan et al., 2021).

The analysis of different articles has shown the issue that personal emotions such as fear, attraction, innocence, greed, or kindness might be exploited to expose sensitive information from the user or rarely to execute financial transactions (Dam et al., 2021). Familiarity with the topic may not bring an advantage in detecting phishing. A person's knowledge of specific topics may indicate additional signs of deception, potentially reducing the cognitive load needed to search for reliable evidence; however, it can also lead to overconfidence and low detection efficiency.

Machine Learning is the almost only way to prevent cyber-attacks

There seems to be a trend towards using machine learning-based approaches to detect ransomware. According to the number of experiments conducted with samples of ransomware, it was noted that more intelligent approaches to detecting and preventing ransomware should be developed. Approaches to detecting ransomware include System Information Analysis, Ransom Note Analysis, File Analysis, Decoys, State Machines, Network Traffic Analysis, and Machine Learning. Approaches to preventing ransomware include Data Backup, Key Management, and User Awareness (Beaman et al., 2021).

Websites or email are the most targeted phishing vectors when developing mitigation strategies

Related to the data analysis, the most targeted phishing vectors for developing mitigation solutions are websites and email. Most existing solutions do not have a specific target area. The solutions are generic. In addition, there are no solutions for eFax and Instant messaging vectors.

4.1.1 Recommendations and guidelines for organizations

The findings for an organization can be divided into 6 categories:

- Training sessions and awareness programs.
- Endpoint security.
- Access control.
- Security policies.
- Polices for devices.
- Generic advice.

Below each section will be explained separately.

Training sessions and awareness programs

Cybersecurity training is the perfect way to raise awareness about common phishing tactics (Touro College Illinois, 2021). An organization must have a training phishing program against phishing (Jampen et al., 2020). Through seminars, conferences, and other virtual learning tools, awareness and teaching programs can be offered. Information programs include conferences, information campaigns, and thematic training. Teaching methods include virtual laboratories, simulators, games, and the use of 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 of training employees needs and what type of training they need (Jampen et al., 2020). However, 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 domains. 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 be able to help people connect the common characteristics of phishing emails (such as action links) to phishing in general. The reason that this allows these features to enhance people's memory of phishing as an alternative explanation. (Wash, 2020).

The best training method 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. (Lim et al., 2021). 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. In addition, if the employee has not clicked on the phishing email, but has not reported it, he should obtain training documents explaining why this step is necessary (Jampen et al., 2020).

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, these mitigation strategies can be done: implement backup strategies; install and update protective software; block pop-ups; update computer hardware (Manjezi, 2019).

Access control

Health institutions are also encouraged to establish and implement appropriate password protection policies and information exchange policies (Argaw et al., 2019). Another article discussed two methods – the web tripwire and the login ritual – 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 (MFA) systems to increase account security in cases of complex phishing attacks. Other authors also suggest the implementation of

Authentication MFA. The MFA will significantly reverse the flow of Office 365 accounts that have been compromised (Moul, 2019).

It can be found that up to 88.2 percent of simulated intruders could be detected using web-based extensions, and half of the participants in Barron's study could perform their rituals every time. They can be deployed in various web applications using popular open-source applications by testing those (Barron et al., 2021).

Security policies

Cybersecurity measures should be based on vulnerability management, potential threats, compromise indicators, and practices in exchange, sharing, and processing of privacy-conscious data (Argaw et al., 2020). In addition, it can be essential to implementing 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).

For the need for authority transfer between multiple teams to find solutions and implement, 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. Having available servers is also useful for supporting employees who are not phishing experts themselves. This solution can also quickly provide a consistent professional recommendation and detailed steps. SS related to phishing is aimed at gratitude to users who reported phishing emails, confirmation that the email is phishing, confirmation that the email is not phishing, assistance to users who clicked on the links, and telling users about the phishing simulation (Althobaiti et al., 2021).

The conclusions described in Abroshan's (2021) paper have an impact on organization security management. For example, assessing the risky behavior of employees of an organization and adapting the company's policy taking into account special training opportunities for security and anti-phishing. There are two options against phishing attacks and their risks to users and employers.

Polices for devices

Recommendations for connected medical devices: Before buying, decision-makers should assess the expected life expectancy of devices (e.g. support from manufacturers/suppliers or support from operating systems). Develop a repair policy to minimize equipment outage time and to ensure timely updates in cooperation with external manufacturing teams. This can allow objects to track new battery alerts to keep up with urgent fixes. Companies should also develop and allocate life cycle management funds to dismantle equipment that cannot be replaced immediately. Maintain a regularly updated registry of every device that is used in the organization (Argaw et al., 2020).

Generic advice

These general tips can be useful for fraudulent calls related to healthcare. People should check all incoming calls for the authorized body. Do not share any information until a call made by another person is expected. This is done to avoid reciprocity. Most attackers continue to attack only those who reciprocate the initial attempts at contact.

In order not to succumb to targeted attack strategies. If a suspicious attempt is made with information about the health status of a person or any member of the family, the attacker may target the victim based on some health information received. Attackers collect information about the targets. This includes both personal information as well as information about their close relatives. This is any information that attackers can get their hands on (Venkatesha et al., 2021). In addition, organizations need to hire cybersecurity professionals (Manjezi and Botha, 2018).

All guidelines and recommendations from the existing literature can be illustrated visually as it is shown in Figure 14 below. To make these points more speaking to the person who is reading it, it is necessary to use personal appeal in verbs.

Figure 14. Recommendations for organizations from SLR

In total, 40 recommendations were created for organizations. In the next subsection, the recommendations for end-users will be developed.

4.1.2 Recommendations and guidelines for end-users

The findings for the end-users can be divided into 2 categories:

- Awareness as the mitigation strategy.
- Security advice.

Below each section will be explained separately.

Awareness as the mitigation strategy

Healthcare organizations are increasingly switching to digital systems, but medical professionals are little aware of the threats. Increased attention to "cyber hygiene" and information management increases awareness of these risks. This highlights the need for, firstly, staff training and awareness, robust firewalls, and implementation policies for IT infrastructure. Hospitals receive a large number of potentially malicious e-mails. Although many employees are aware of phishing and appear to react accordingly, continuous training throughout the cybersecurity field is required (Priestman et al., 2019).

The following methods against phishing attacks can be used for end-users: use a phishing list of browsers; use sites to test links; use your skills to prevent cyber-attacks (Venkatesha et al., 2021). Other suggestions from the phishing prevention literature: think before clicking; install a phishing anti-attack toolbar; keep the browser up-to-date, use firewalls, check site security; be careful of pop-ups, do not share personal information; use antivirus software (Sadiq et al., 2021). The author Argaw (2019) stated that end-users should not use the same password on multiple accounts. In addition, they should not keep computers unsupervised and trust suspicious emails.

According to Jampen (2020), the user parameters down below affect the susceptibility to phishing and the type of training that gives efficient results.

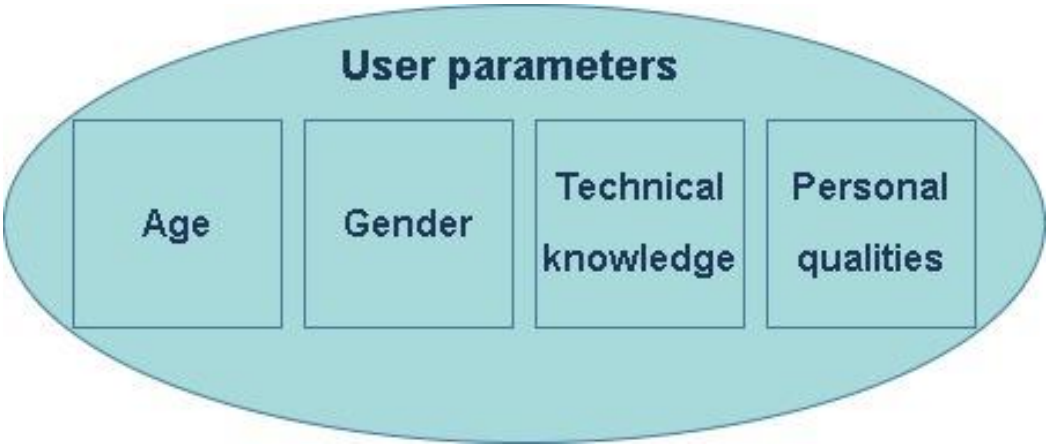

Figure 15. User parameters.

If taking into consideration these parameters, it will be good for users to gain more technical knowledge.

Security advice

People should be more attentive to their computer security. For example, they should avoid using public computers to interact with confidential information. It will be good if users maintain antivirus software and update programs regularly. They need to take special care with emails of questionable origin. For instance, if a user finds an email of unknown origin and it seems to him that this is an email with a virus, then he should delete it without opening it (Jampen et al., 2020).

Strong authentication can protect users from many identity attacks, reducing the probability of security breaches. To ensure the best protection and user experience, it is recommended to use authentication options without a password. The preferred option for SMS / Voice authentication is always to use an authentication application (Venkatesha et al., 2021). End users should check whether the web pages they visit are completely reliable and whether they have a security certificate. Moreover, the website address usually should start with HTTP://. If a person has doubts, the user should seek help from a specialist in this field (Jampen et al., 2020).

All guidelines and recommendations for end-users from the existing literature can be illustrated visually as it is shown in Figure 16 below.

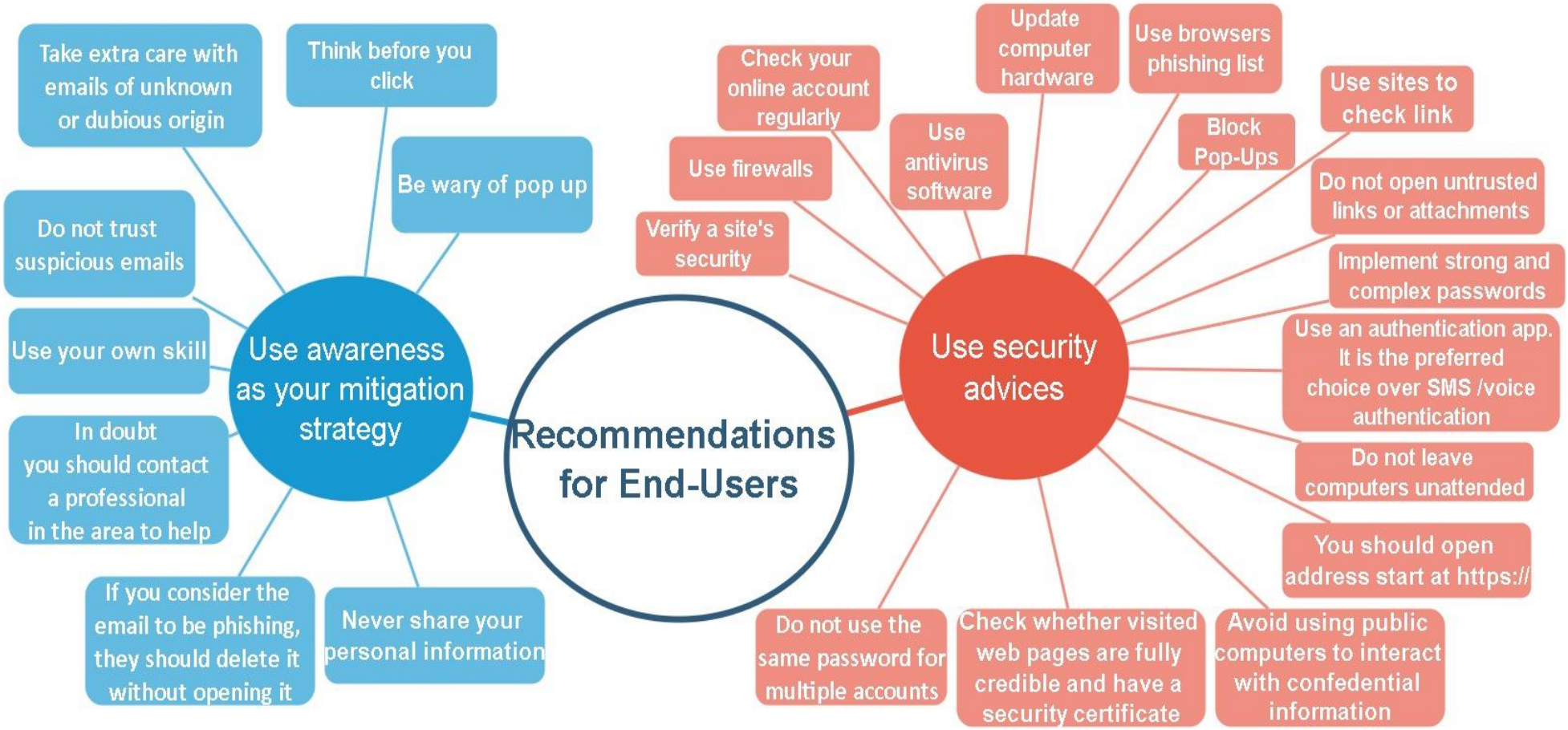

Figure 16. Recommendations for end-users from SLR.

In total, 24 recommendations were created for end-users.

4.2 Development of a co-design workshop

This thesis does not limit to just identifying the existing recommendations and best practices but proposes an approach to identify more guidelines and best practices by following a participatory approach involving researchers, technologists, and developers to take a part in it.

4.2.1 Preparation for the workshop

Below are the suggestions of what to do before conducting the co-design workshop. The idea suggestions were taken from Medium (2016).

Table 10. Tips for conducting a co-design workshop

Tips	Description
Workshop agenda	It determines the activities to be developed, the adaptation to a particular context, and the end assessment. The program defines the number of activities to be developed.
The right invitation	It is more than an appointment; it is an invitation for people to spend their time and energy in a way that can be very different from anything they have experienced in their life. Therefore, try to talk to people about the workshop in real-time.
Training materials	These include visual aids, presentations, slides, manuals, etc.
The right space	Using the same old boardroom to host these seminars may give the wrong impression that this is business as usual. The best option will be to find an open, spacious, natural lightroom, with plenty of space on the wall.

Production Needs	A list of production needs for workshops, including food, specific needs, transportation, digital communication infrastructure, etc.
Snacking	Take care of people's physical needs to prepare them to contribute. Coffee and semi-finished products are the fuel for the workshop.
Timer	A time tracking mechanism accurate to the minute will be crucial to maintain momentum.
Noise source	Determined by the number of participants and the size of the room, there may be a need to signal the moment when attention should be drawn back to the front of the room.
Training tools	The workshop will use methods, games, energy exercises, role-play activities, and prototype techniques. List the materials required for the implementation of these methods.

Co-design workshops can be organized with a single participant or a group of them because of the practical nature of these courses, mixed groups of users, designers, and researchers can achieve important results and contribute to the coordination of user-oriented processes in the company. Nevertheless, a researcher must continue to lead sessions and teach team members how best to interact with participants, for example, what types of questions to ask, and what language to use (UX Magazine, 2012).

4.2.2 Proposed workshop structure

If a person is working with large group attendees, the group should be divided into three subgroups and monitor as much as possible their work and internal discussions. Each subgroup can work on the same or different topics and present their work at the end of the meeting to the other groups.

Most workshops on collaborative design last 1.5-2 hours, although some may be longer. The conversation usually begins with a study of the results of research exercises on self-reflection performed at the first stage and is accompanied by one or more practical

exercises. The structure illustrated below shows the main three phases of a co-design workshop (Co-create, 2019).

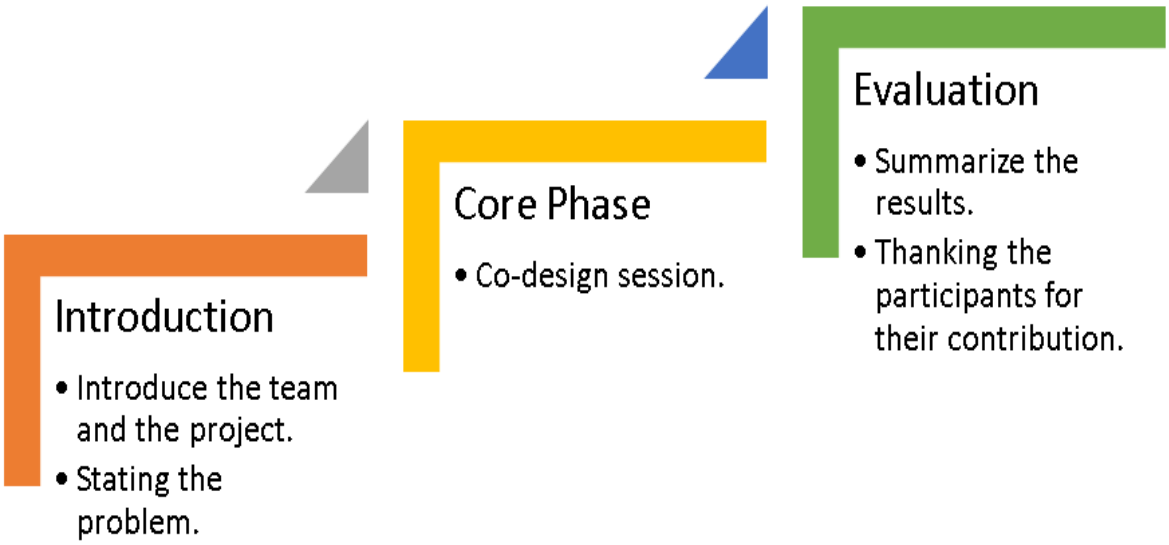

Figure 17. The proposed structure.

Phase 1. Introduction

The first phase starts with introducing the team and the project itself. The team should tell the structure for the session to the participants, so they know to expect what will be in a co-design session. Include a description of the purpose of the session and outline the goals and value of the activities. It is also recommended to provide brief background information to the participants, so they know what problems they are designed for.

Phase 2. Core Phase

This stage includes running the co-design session with different co-design activities. The proposed activities for it are represented below:

- Map-it.
- Storytelling.
- Evaluation Matrix.

Map-it is a participatory mapping method, used to enable the visualization of a process openly and flexibly. It uses a series of icons that allow participants from different backgrounds to participate equally in a process of co-creation by expressing themselves clearly and visually. This methodology can be used for various purposes, such as co-creation of ideas, concept evaluation, decomposition of complex structures and concepts,

participation, and equal participation of people. As in the World Café activity, participants can discuss issues in small groups around cafeteria tables. Storytelling is an activity that helps to share knowledge, establish a new understanding, and stimulate people to participate actively. This is done because stories can attract and keep the attention and increase the chances of the participants of a workshop contributing to a process of co-creation. The Evaluation Matrix is based on the most relevant success criteria of the project to prioritize ideas. Well-defined examples and demonstrations for any specific activities used should be provided so that people are clear about what they will be doing during the exercise (CIPTEC, 2018).

Phase 3. Evaluation

After the workshop was held, it is recommended to follow these steps:

- Write it: Before anything on the walls is removed, ensure that each drawing is documented and photographed.
- Develop it: Plan an independent time for designers and design teams to combine the design with the recommendations. This advice can be given in a more precise form in wireframes and design.
- Discuss it: The design recommendations contain many familiar elements created during the workshop, which will form the basis for further reflection and discussion.
- Try it: It is recommended to obtain feedback from users before drafting and developing processes.

After discussing the proposed methods in this part of the thesis, further, there is the discussion section.

5 Discussion

This section provides a discussion of the results of the research and answers to the questions raised during the thesis. The following sub-research questions were answered:

What are the identified prevention mechanisms reported in the literature?

Talking about the first research question, it should be considered that this research question was solved by conducting a systematic literature review. Systematic Literature Review (SLR) was implemented for reviewing 158 primary studies that were selected after searching the related literature published over the last 3 years (2019–March 2022). The following scientific databases were used to collect and analyze data: Springer, IEEE, ACM, Web of Science, and Scopus. The systematic literature review additionally answers the research questions designed specifically for it, which are described in the methodology part. It helped to identify guidelines and best practices from the existing literature on how to prevent phishing and ransomware attacks.

How can the existing solutions be classified and visually represented?

To propose the classification of existing solutions for the prevention of phishing and ransomware attacks in the healthcare sector, an attempt of systematic literature review had been made. Based on its analysis, it was defined that the visual presentation of the recommendations can be easier to perceive and more catchy. Overall, 40 recommendations for organizations and 24 recommendations for end-users were defined. The findings are not limited to one healthcare sphere but apply to every sector that needs to implement these recommendations against cyber-attacks.

Is there a way to supplement the recommendations from the literature?

In answering this research question, it was found that participatory research consists of different approaches, and conducting a co-design workshop can be a good way to bring more guidelines and recommendations. Therefore, people’s experiences and thoughts of

co-design participants can be combined with theoretical knowledge from the systematic literature review. In the thesis, a plan and proposed methods for a co-design workshop with the representatives of the cyber-security industry were presented.

Based on the discussion of sub-research questions, the main research questions can be answered:

What are the prevention mechanisms against phishing and ransomware attacks?

All prevention mechanisms against phishing and ransomware attacks were identified in this thesis from the theoretical perspective of the related literature. The existing solutions can be classified into nine categories. The results part of this work explained them in more detail. The proposed solutions for mitigating cyber-attacks have mostly generic target areas, but can be applied to the organizations and end-users. The main vectors that were chosen to develop these solutions were associated with websites and email. A prevalent amount of the solutions were built upon machine learning algorithms.

6. Conclusion

The healthcare sector develops every day as a part of global digitalization. Moreover, health data are very valuable as potential targets for hackers. Phishing is malicious exploitation that uses targeted communication. To answer the research questions that were discussed in the thesis, empirical papers from various fields have been collected and summarized. The importance of preventing phishing and ransomware attacks was explained. According to the results of the systematic literature review ontologies of recommendations for target groups as organizations and end-users were presented. Taken together, these results demonstrate that there is a need for developing more solutions against cyber-attacks. The presented findings have the potential to assist in preventing phishing and ransomware attacks for an organization that wishes to develop its protection mechanisms accordingly The most important limitation lies in the fact that only the newest articles were explored in this thesis.

Future research should consider the potential effects of created guidelines and recommendations. Future work on the thesis topic can be connected with conducting a co-design workshop on proposed methods. It can be done to synthesize new knowledge on how to prevent phishing and ransomware attacks. The created recommendations from this thesis can be represented there as material for corrections and future development. Research into solving this problem is already in progress.

References

Abbas, S. et al. (2021) ‘Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach’, Sensors, 21. doi:10.3390/s21144816.

Abdulhamid, S., Gana, N., and Shafi, • (2020) Machine Learning Classification Algorithms for Phishing Detection: A Comparative Appraisal and Analysis. doi:10.1109/NigeriaComputConf45974.2019.8949632.

Abroshan, H. et al. (2021a) A phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks, p. 350. doi:10.1145/3450614.3464472.

Abroshan, H. et al. (2021b) ‘Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process’, IEEE Access, 9, pp. 44928–44949. doi:10.1109/ACCESS.2021.3066383.

Adebowale, M. and Lwin, K. (2019) Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection. doi:10.1109/SKIMA47702.2019.8982427.

Adebowale, M. et al. (2018) ‘Intelligent Web-Phishing Detection and Protection Scheme using integrated Features of Images, Frames and Text’, Expert Systems with Applications, 115, pp. 300–313. doi:10.1016/j.eswa.2018.07.067.

Adebowale, M.A., Lwin, K.T. and Hossain, M.A. (2020) ‘Intelligent phishing detection scheme using deep learning algorithms’, Journal of Enterprise Information Management, ahead-of-print(ahead-of-print). doi:10.1108/JEIM-01-2020-0036.

Adil, M. et al. (2020) Preventive Techniques of Phishing Attacks in Networks. doi:10.1109/ICACS47775.2020.9055943.

Al-Fayoumi, M., Alwidian, J. and Abusaif, M. (2019) ‘Intelligent Association Classification Technique for Phishing Website Detection’, International Arab Journal of Information Technology, 17. doi:10.34028/iajit/17/4/7.

Alhamad, H., Alzyadh, T. and Badawi, M. (2020) ‘Detecting E-Banking Phishing Website using C4.5 Algorithm’, p. 46. doi:10.22937/IJCSNS.2020.20.11.6.

Al-hamar, Y. and Kolivand, H. (2020) A New Email Phishing Training Website, p. 268. doi:10.1109/DeSE51703.2020.9450238.

Al-Hamar, Y. et al. (2021) ‘Enterprise Credential Spear-phishing attack detection’, Computers & Electrical Engineering, 94, p. 107363. doi:10.1016/j.compeleceng.2021.107363.

Aljofey, A. et al. (2020) ‘An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL’, Electronics, 9, p. 1514. doi:10.3390/electronics9091514.

Alkawaz, M. et al. (2021) A Comprehensive Survey on Identification and Analysis of Phishing Website based on Machine Learning Methods, p. 87. doi:10.1109/ISCAIE51753.2021.9431794.

Almeida, R. and Westphall, C. (2020) ‘Heuristic Phishing Detection and URL Checking Methodology Based on Scraping and Web Crawling’, in 2020 IEEE International Conference on Intelligence and Security Informatics (ISI). 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1–6. doi:10.1109/ISI49825.2020.9280549.

Alotaibi, R., Al-Turaiki, I. and Alakeel, F. (2020) ‘Mitigating Email Phishing Attacks using Convolutional Neural Networks’, in 2020 3rd International Conference on Computer Applications Information Security (ICCAIS). 2020 3rd International Conference on Computer Applications Information Security (ICCAIS), pp. 1–6. doi:10.1109/ICCAIS48893.2020.9096821.

Alsariera, Y.A., Elijah, A.V. and Balogun, A.O. (2020) ‘Phishing Website Detection: Forest by Penalizing Attributes Algorithm and Its Enhanced Variations’, Arabian Journal for Science and Engineering, 45(12), pp. 10459–10470. doi:10.1007/s13369-020-04802-1.

Althobaiti, K., Jenkins, A.D.G., and Vaniea, K. (2021) ‘A Case Study of Phishing Incident Response in an Educational Organization’, Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), pp. 1–32. doi:10.1145/3476079.

Alzamil, Z. et al. (2020) ‘A HYBRID PHISHING DETECTION APPROACH FOR MOBILE APPLICATION’, International Journal of Security and its Applications, 14, pp. 15–28. doi:10.33832/ijsia.2020.14.3.02.

Arduin, P.-E., de Oliveira, K.M. and Kolski, C. (2021) ‘Trust me and Click! A Pilot Study of Cognitive Walkthrough for Phishing Emails’, in 2021 14th International Conference on Human System Interaction (HSI). 2021 14th International Conference on Human System Interaction (HSI), pp. 1–6. doi:10.1109/HSI52170.2021.9538649.

Argaw, S.T. et al. (2019) ‘The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review’, BMC Medical Informatics and Decision Making, 19(1), p. 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 Medical Informatics and Decision Making, 20(1), p. 146. doi:10.1186/s12911-020-01161-7.

Ariyadasa, S., Fernando, Subha and Fernando, Shantha (2020) ‘Detecting phishing attacks using a combined model of LSTM and CNN’, International Journal of ADVANCED AND APPLIED SCIENCES, 7, pp. 56–67. doi:10.21833/ijaas.2020.07.007.

Athulya, A. and Praveen, K. (2020) ‘Towards the Detection of Phishing Attacks’, 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) [Preprint]. doi:10.1109/ICOEI48184.2020.9142967.

Aung, E.S. and Yamana, H. (2019) ‘URL-based Phishing Detection using the Entropy of Non-Alphanumeric Characters’, in Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services. iiWAS2019: The 21st International Conference on Information Integration and Web-based Applications & Services, Munich Germany: ACM, pp. 385–392. doi:10.1145/3366030.3366064.

Awasthi, A. and Goel, N. (2021) Generating Rules to Detect Phishing Websites Using URL Features, p. 9. doi:10.1109/ODICON50556.2021.9429003.

Azeez, N.A. et al. (2021) 'Adopting automated whitelist approach for detecting phishing attacks', Computers & Security, 108, p. 102328. doi:10.1016/j.cose.2021.102328.

Baillon, A. et al. (2019) 'Informing, simulating experience, or both: A field experiment on phishing risks', PLoS ONE, 14(12), p. e0224216. doi:10.1371/journal.pone.0224216.

Balogun, A. et al. (2021) 'Rotation Forest-Based Logistic Model Tree for Website Phishing Detection', in, pp. 154–169. doi:10.1007/978-3-030-87013-3_12.

Barron, T., So, J. and Nikiforakis, N. (2021) 'Click This, Not That: Extending Web Authentication with Deception', in Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security. New York, NY, USA: Association for Computing Machinery, pp. 462–474. Available at: http://doi.org/10.1145/3433210.3453088 (Accessed: 27 April 2022).

Bathala, H.V. et al. (2021) 'Zero-Day attack prevention Email Filter using Advanced Machine Learning ', in 2021 5th Conference on Information and Communication Technology (CICT). 2021 5th Conference on Information and Communication Technology (CICT), pp. 1–6. doi:10.1109/CICT53865.2020.9672420.

Beaman, C. et al. (2021) 'Ransomware: Recent advances, analysis, challenges, and future research directions', Computers & Security, 111, p. 102490. doi:10.1016/j.cose.2021.102490.

Becker's Healthcare. The first known ransomware attack in 1989 also targeted healthcare (2016). Available at: https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html (Accessed: 26 April 2022).

Bhardwaj, A. et al. (2021) 'Privacy-aware detection framework to mitigate new-age phishing attacks', Computers & Electrical Engineering, 96, p. 107546. doi:10.1016/j.compeleceng.2021.107546.

Bhoj, N. et al. (2021) ‘Naive and Neighbour Approach for Phishing Detection, in 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT). 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 171–175. doi:10.1109/CSNT51715.2021.9509566.

Bikov, T.D. et al. (2019) ‘Phishing in Depth – Modern Methods of Detection and Risk Mitigation ’, in 2019 42nd International Convention on Information and Communication Technology, Electronics, and Microelectronics (MIPRO). 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 447–450. doi:10.23919/MIPRO.2019.8757074.

Boukari, B.E., Ravi, A. and Msahli, M. (2021) ‘Machine Learning Detection for SMiShing Frauds’, in 2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC). 2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC), pp. 1–2. doi:10.1109/CCNC49032.2021.9369640.

Bountakas, P., Koutroumpouchos, K. and Xenakis, C. (2021) A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection, p. 12. doi:10.1145/3465481.3469205.

Bozkir, A. and Aydos, M. (2020) ‘LogoSENSE: A Companion HOG based Logo Detection Scheme for Phishing Web Page and E-mail Brand Recognition’, Computers & Security, 95. doi:10.1016/j.cose.2020.101855.

Brites, D. and Wei, M. (2019) ‘PhishFry - A Proactive Approach to Classify Phishing Sites Using SCIKIT Learn’, in 2019 IEEE Globecom Workshops (GC Wkshps). 2019 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. doi:10.1109/GCWkshps45667.2019.9024428.

Burda, P., Allodi, L. and Zannone, N. (2020) ‘Don’t Forget the Human: a Crowdsourced Approach to Automate Response and Containment Against Spear Phishing Attacks’, in 2020 IEEE European Symposium on Security and Privacy

Workshops (EuroS PW). 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 471–476. doi:10.1109/EuroSPW51379.2020.00069.

Butt, M.H.F. et al. (2021) 'Intelligent Phishing Url Detection: A Solution Based On Deep Learning Framework', in 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 434–439. doi:10.1109/ICCWAMTIP53232.2021.9674162.

Cernica, I. and Popescu, N. (2020) Computer Vision-Based Framework For Detecting Phishing Webpages, p. 4. doi:10.1109/RoEduNet51892.2020.9324850.

Chen, Y.-H. and Chen, J.-L. (2019) 'AI@ntiPhish — Machine Learning Mechanisms for Cyber-Phishing Attack', IEICE Transactions on Information and Systems, E102.D(5), pp. 878–887. doi:10.1587/transinf.2018NTI0001.

Cho, H., Bartlett, G., and Freedman, M. (2021) Agenda Pushing in Email to Thwart Phishing, p. 118. doi:10.18653/v1/2021.dialdoc-1.15.

CIPTEC. D3.3: Plan for co-creation/co-design workshops (2018) Horizon 2020 project. Available at: http://ciptec.eu/download/d3-3-plan-for-co-creationco-design-workshops/ (Accessed: 25 May 2022).

Co-create (2019) 'The Co-Create Handbook for Creative Professionals', CO-CREATION SKILLS & TRAINING, 15 March. Available at: http://www.cocreate.training/2019/03/15/the-co-create-handbook-for-creative-professionals/ (Accessed: 25 May 2022).

Co-design: A Powerful Force for Creativity and Collaboration | by Stratos Innovation Group | Medium (no date). Available at: https://medium.com/@thestratosgroup/co-design-a-powerful-force-for-creativity-and-collaboration-bed1e0f13d46 (Accessed: 26 April 2022).

Cornwall, A., & Jewkes, R. (1995). What is participatory research? Social Science & Medicine, 41(12), 1667–1676. https://doi.org/10.1016/0277-9536(95)00127-s

Cuchta, T. et al. (2019) Human Risk Factors in Cybersecurity, p. 92. doi:10.1145/3349266.3351407.

Cui, Q. et al. (2021) ‘Proactive Detection of Phishing Kit Traffic’, in, pp. 257–286. doi:10.1007/978-3-030-78375-4_11.

Cyber attack could cost Sony studio as much as $100 million | Reuters (no date). Available at: https://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209 (Accessed: 26 April 2022).

Cyberattacks 2021: Statistics From the Last Year (2022) Spanning. Available at: https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/ (Accessed: 26 April 2022).

Cybersecurity: main and emerging threats in 2021 (infographic) | News | European Parliament (2022). Available at: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic (Accessed: 26 April 2022).

Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. (2021) ‘Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks’, Education and Information Technologies [Preprint]. doi:10.1007/s10639-021-10806-7.

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

Datta, P. et al. (2021) ‘Warning users about cyber threats through sounds’, SN Applied Sciences, 3(7), p. 714. doi:10.1007/s42452-021-04703-4.

De La Torre Parra, G. et al. (2020) ‘Detecting Internet of Things attacks using distributed deep learning’, Journal of Network and Computer Applications, 163, p. 102662. doi:10.1016/j.jnca.2020.102662.

Derakhshan, A., Harris, I. and Behzadi, M. (2021) Detecting Telephone-based Social Engineering Attacks using Scam Signatures, p. 73. doi:10.1145/3445970.3451152.

Designing a co-design workshop. The why, the what, and the how | by Gyöngyi Fekete | Medium (no date). Available at: https://medium.com/@gyngyifekete/designing-a-co-design-workshop-7686eaf4bf0f (Accessed: 26 April 2022).

Desolda, G. et al. (2019) 'Alerting Users About Phishing Attacks', in, pp. 134–148. doi:10.1007/978-3-030-22351-9_9.

Detecting CryptoWall 3.0 Using Real Time Event Correlation (2015) Digital Guardian. Available at: https://digitalguardian.com/blog/detecting-cryptowall-3-using-real-time-event-correlation (Accessed: 25 May 2022).

Drichel, A. et al. (2021) Finding Phish in a Haystack: A Pipeline for Phishing Classification on Certificate Transparency Logs, p. 12. doi:10.1145/3465481.3470111.

Dukarm, C., Dill, R. and Reith, M. (2019) 'Improving Phishing Awareness in the United States Department of Defense', in Cruz, T. and 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: http://www.webofscience.com/wos/woscc/full-record/WOS:000560821500021 (Accessed: 20 May 2022).

E, M., and A, K. (2019) 'New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing ', Security and Communication Networks, 2019, pp. 1–11. doi:10.1155/2019/5141395.

ENISA Threat Landscape 2021 (no date) ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (Accessed: 26 April 2022).

European Commission. (2021) A cyber-secure digital transformation in a complex threat environment — Brochure | Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure (Accessed: 26 April 2022).

ExtraHop. How Does Ransomware Work? (2022). Available at: https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/ (Accessed: 26 April 2022).

F.B.I. Director Compares Ransomware Danger to 9/11 Threat - The New York Times (no date). Available at: https://www.nytimes.com/2021/06/04/us/politics/ransomware-cyberattacks-sept-11-fbi.html (Accessed: 26 April 2022).

Feng, T. and Yue, C. (2020) Visualizing and Interpreting RNN Models in URL-based Phishing Detection, p. 24. doi:10.1145/3381991.3395602.

Fetooh, H.T.M., El-Gayar, M.M. and Aboelfetouh, A. (2021) 'Detection Technique and Mitigation Against a Phishing Attack', International Journal of Advanced Computer Science and Applications, 12(9). doi:10.14569/IJACSA.2021.0120922.

Fouss, B. et al. (2019) 'PunyVis: A Visual Analytics Approach for Identifying Homograph Phishing Attacks', in 2019 IEEE Symposium on Visualization for Cyber Security (VizSec). 2019 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–10. doi:10.1109/VizSec48167.2019.9161590.

Gomes, V., Reis, J. and Alturas, B. (2020) 'Social Engineering and the Dangers of Phishing', in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–7. doi:10.23919/CISTI49556.2020.9140445.

Guo, B. et al. (2021) 'HinPhish: An Effective Phishing Detection Approach Based on Heterogeneous Information Networks', Applied Sciences, 11, p. 9733. doi:10.3390/app11209733.

Halgaš, L., Agrafiotis, I. and Nurse, J. (2020) 'Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)', in, pp. 219–233. doi:10.1007/978-3-030-39303-8_17.

Haney, O. and Elaarag, H. (2021) Secure Suite: An Open-Source Service for Internet Security, p. 7. doi:10.1109/SoutheastCon45413.2021.9401865.

Healthcare expenditure statistics (2021). Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics (Accessed: 26 April 2022).

Helmi, R. et al. (2019) Email Anti-Phishing Detection Application, p. 267. doi:10.1109/ICSEngT.2019.8906316.

Higashino, M. (2019) A Design of an Anti-Phishing Training System Collaborated with Multiple Organizations, p. 592. doi:10.1145/3366030.3366086.

Higashino, M. et al. (2019) An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage, p. 86. doi:10.1109/INFOMAN.2019.8714691.

Hr, M.G. et al. (2020) 'Development of anti-phishing browser based on random forest and rule of extraction framework', Cybersecurity, 3(1), p. 20. doi:10.1186/s42400-020-00059-1.

Huang, Yongjie, et al. (2019) Phishing URL Detection via CNN and Attention-Based Hierarchical RNN, p. 119. doi:10.1109/TrustCom/BigDataSE.2019.00024.

Huang, Yuankun, et al. (2019) 'VPCID—A VoIP Phone Call Identification Database', in Yoo, C.D. et al. (eds) Digital Forensics and Watermarking. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 307–321. doi:10.1007/978-3-030-11389-6_23.

IBM (2022) IBM Security X-Force Threat Intelligence Index. Available at: https://www.ibm.com/security/data-breach/threat-intelligence/www.ibm.com/security/data-breach/threat-intelligence (Accessed: 26 April 2022).

IBM Security Services. (2014). IBM security services 2014 cyber security intelligence index: Analysis of cyber-attack and incident data from IBM's worldwide security operations (Report No. SE303058-USEN-02). Somers, NY: IBM Corporation.

Insurance giant AXA victim of ransomware attack | 2021-05-19 | Security Magazine (no date). Available at: https://www.securitymagazine.com/articles/95245-insurance-giant-axa-victim-of-ransomware-attack (Accessed: 26 April 2022).

Intelligence, I. (no date) The Digital Health Ecosystem 2022: How COVID changed the US healthcare system, Insider Intelligence. Available at: https://www.insiderintelligence.com/insights/digital-health-ecosystem/ (Accessed: 26 April 2022).

Irwin, L. (2021) The 5 biggest ransomware pay-outs of all time, IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/the-5-biggest-ransomware-pay-outs-of-all-time (Accessed: 26 April 2022).

Ishikawa, T. et al. (2020) 'Machine learning for tree structures in fake site detection', in Proceedings of the 15th International Conference on Availability, Reliability, and Security. ARES 2020: The 15th International Conference on Availability, Reliability, and Security, Virtual Event Ireland: ACM, pp. 1–10. doi:10.1145/3407023.3407035.

Islam, R. et al. (2021) 'LinkMan: hyperlink-driven misbehavior detection in online security forums', in Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. ASONAM '21: International Conference on Advances in Social Networks Analysis and Mining, Virtual Event Netherlands: ACM, pp. 270–277. doi:10.1145/3487351.3488323.

Ismail, S., Alkawaz, M.H. and Kumar, A.E. (2021) 'Quick Response Code Validation and Phishing Detection Tool', in 2021 IEEE 11th IEEE Symposium on Computer Applications Industrial Electronics (ISCAIE). 2021 IEEE 11th IEEE Symposium on Computer Applications Industrial Electronics (ISCAIE), pp. 261–266. doi:10.1109/ISCAIE51753.2021.9431807.

Jain, A.K. and Gupta, B.B. (2019) 'A machine learning-based approach for phishing detection using hyperlinks information', Journal of Ambient Intelligence and Humanized Computing, 10(5), pp. 2015–2028. doi:10.1007/s12652-018-0798-z.

Jampen, D. et al. (2020) ‘Don’t click: towards an effective anti-phishing training. A comparative literature review’, Human-centric Computing and Information Sciences, 10(1), p. 33. doi:10.1186/s13673-020-00237-7.

Jr, R.W. (2021) ‘Cyber Threat Alert: Ransomware Breaks Another Record’, SonicWall, 28 October. Available at: https://testmerge-blog.dev.swweb.app/en-us/2021/10/cyber-threat-alert-ransomware-breaks-another-record/ (Accessed: 26 April 2022).

Kardaş, B. et al. (2021) ‘Detecting spam tweets using machine learning and effective preprocessing’, in Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. ASONAM ’21: International Conference on Advances in Social Networks Analysis and Mining, Virtual Event Netherlands: ACM, pp. 393–398. doi:10.1145/3487351.3490968.

Kasim, Ö. (2021) ‘Automatic detection of phishing pages with event-based request processing, deep-hybrid feature extraction, and light gradient boosted machine model’, Telecommunication Systems, 78(1), pp. 103–115. doi:10.1007/s11235-021-00799-6.

Khan, W. et al. (2021) ‘SpoofCatch: A Client-Side Protection Tool Against Phishing Attacks’, IT Professional, 23(2), pp. 65–74. doi:10.1109/MITP.2020.3006477.

Korkmaz, M. et al. (2021) ‘Deep Neural Network Based Phishing Classification on a High-Risk URL Dataset’, in, pp. 648–657. doi:10.1007/978-3-030-73689-7_62.

Korkmaz, M., Sahingoz, O. and Diri, B. (2020) Detection of Phishing Websites by Using Machine Learning-Based URL Analysis, p. 7. doi:10.1109/ICCCNT49239.2020.9225561.

Kraus, S. et al. (2021) ‘Digital Transformation: An Overview of the Current State of the Art of Research’, SAGE Open, 11(3), p. 21582440211047576. doi:10.1177/21582440211047576.

Kumar, J. et al. (2020) Phishing Website Classification and Detection Using Machine Learning, p. 6. doi:10.1109/ICCCI48352.2020.9104161.

Kumar, V. and Sinha, D. (2021) ‘A robust intelligent zero-day cyber-attack detection technique’, Complex & Intelligent Systems, 7(5), pp. 2211–2234. doi:10.1007/s40747-021-00396-9.

Lam, T. and Kettani, H. (2019) ‘PhAttApp: A Phishing Attack Detection Application’, in Proceedings of the 2019 3rd International Conference on Information System and Data Mining - ICISDM 2019. the 2019 3rd International Conference, Houston, TX, USA: ACM Press, pp. 154–158. doi:10.1145/3325917.3325927.

Lambat, Y. et al. (2021) ‘A Mamdani Type Fuzzy Inference System to Calculate Employee Susceptibility to Phishing Attacks’, Applied Sciences, 11, p. 1. doi:10.3390/app11199083.

Le Page, S. and Jourdan, G.-V. (2019) ‘Victim or Attacker? A Multi-dataset Domain Classification of Phishing Attacks’, in 2019 17th International Conference on Privacy, Security, and Trust (PST). 2019 17th International Conference on Privacy, Security, and Trust (PST), pp. 1–10. doi:10.1109/PST47121.2019.8949038.

Lee, C.S. (2020) ‘A crime script analysis of transnational identity fraud: migrant offenders’ use of technology in South Korea’, Crime, Law and Social Change, 74(2), pp. 201–218. doi:10.1007/s10611-020-09885-3.

Li, J., Zhang, Z. and Guo, C. (2021) ‘Machine Learning-Based Malicious X.509 Certificates’ Detection’, Applied Sciences, 11, p. 2164. doi:10.3390/app11052164.

Liew, S.W. et al. (2019) ‘An effective security alert mechanism for real-time phishing tweet detection on Twitter’, Computers & Security, 83, pp. 201–207. doi:10.1016/j.cose.2019.02.004.

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

Lin, Y. et al. (no date) ‘Phishpedia: A Hybrid Deep Learning-Based Approach to Visually Identify Phishing Webpages’, p. 19.

Listík, V. et al. (2019) ‘Phishing Email Detection based on Named Entity Recognition’:, in Proceedings of the 5th International Conference on Information Systems Security and Privacy. 5th International Conference on Information Systems Security and Privacy, Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, pp. 252–256. doi:10.5220/0007314202520256.

Liu, D. et al. (2019) PhishLedger: A Decentralized Phishing Data Sharing Mechanism, IECC ’19: Proceedings of the 2019 International Electronics Communication Conference, p. 89. doi:10.1145/3343147.3343154.

Luh, R. et al. (2020) ‘PenQuest: a gamified attacker/defender meta-model for cyber security assessment and education’, Journal of Computer Virology and Hacking Techniques, 16(1), pp. 19–61. doi:10.1007/s11416-019-00342-x.

M, Y., Janet, B. and Reddy, U.S. (2020) Anti-phishing System using LSTM and CNN, p. 5. doi:10.1109/INOCON50539.2020.9298298.

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.

Manyumwa, T. et al. (2020) ‘Towards Fighting Cybercrime: Malicious URL Attack Type Detection using Multiclass Classification’, in 2020 IEEE International Conference on Big Data (Big Data). 2020 IEEE International Conference on Big Data (Big Data), pp. 1813–1822. doi:10.1109/BigData50022.2020.9378029.

Mao, J. et al. (2019) ‘Phishing page detection via learning classifiers from page layout feature’, EURASIP Journal on Wireless Communications and Networking, 2019(1), p. 43. doi:10.1186/s13638-019-1361-0.

Martins de Souza, C.H. et al. (2020) ‘On detecting and mitigating phishing attacks through featureless machine learning techniques’, Internet Technology Letters, 3(1), p. e135. doi:10.1002/itl2.135.

Maurya, S., Singh, H. and Jain, A. (2019) ‘Browser Extension based Hybrid Anti-Phishing Framework using Feature Selection’, International Journal of Advanced Computer Science and Applications, 10(11). doi:10.14569/IJACSA.2019.0101178.

Megha, N., Raman, K.R.R. and Sherly, E. (2019) An Intelligent System for Phishing Attack Detection and Prevention, p. 1582. doi:10.1109/ICCES45898.2019.9002204.

Miao, M. and Wu, B. (2020) 'A Flexible Phishing Detection Approach Based on Software-Defined Networking Using Ensemble Learning Method', in Proceedings of the 2020 4th International Conference on High-Performance Compilation, Computing and Communications. HP3C 2020: 2020 4th International Conference on High-Performance Compilation, Computing, and Communications, Guangzhou China: ACM, pp. 70–73. doi:10.1145/3407947.3407952.

Mishra, S. and Soni, D. (2021) 'DSmishSMS-A System to Detect Smishing SMS', Neural Computing and Applications [Preprint]. doi:10.1007/s00521-021-06305-y.

Mitchell H. (2021) J&J experiences 15.5B cybersecurity incidents per day, CISO says. Available at: https://www.beckershospitalreview.com/cybersecurity/j-j-experiences-15-5b-cybersecurity-incidents-per-day-ciso-says.html (Accessed: 26 April 2022).

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.

Mridha, K. et al. (2021) 'Phishing URL Classification Analysis Using ANN Algorithm', in 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON). 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), pp. 1–7. doi:10.1109/GUCON50781.2021.9573797.

Mukhopadhyay, A. and Prajwal, A. (2021) EDITH - A Robust Framework for Prevention of Cyber Attacks in the Covid Era, p. 8. doi:10.1109/INCET51464.2021.9456186.

Naaz, S. (2021) 'Detection of Phishing in the Internet of Things Using Machine Learning Approach', International Journal of Digital Crime and Forensics, 13, pp. 1–15. doi:10.4018/IJDCF.2021030101.

Nabeel, M. et al. (2020) ‘Following Passive DNS Traces to Detect Stealthy Malicious Domains Via Graph Inference’, ACM Transactions on Privacy and Security, 23, pp. 1–36. doi:10.1145/3401897.

Nathezhtha, T., Sangeetha, D. and Vaidehi, V. (2019) ‘WC-PAD: Web Crawling based Phishing Attack Detection’, in 2019 International Carnahan Conference on Security Technology (ICCST). 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1–6. doi:10.1109/CCST.2019.8888416.

NBC News. A baby died because of a ransomware attack on the hospital, the suit says (2021). Available at: https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 (Accessed: 26 April 2022).

Ndagi, J.Y., and Alhassan, J.K. (2019) ‘Machine Learning Classification Algorithms for Adware in Android Devices: A Comparative Evaluation and Analysis’, in 2019 15th International Conference on Electronics, Computer, and Computation (ICECCO). 2019 15th International Conference on Electronics, Computer, and Computation (ICECCO), pp. 1–6. doi:10.1109/ICECCO48375.2019.9043288.

Nik Aein Koupaei, A. and Nazarov, A. (2020) A Hybrid Security Solution for Mitigating Cyber-Attacks on Info-Communication Systems, p. 4. doi:10.1109/EnT50437.2020.9431296.

Nirmal, K., Janet, B. and Kumar, R. (2021) ‘Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection’, Peer-to-Peer Networking and Applications, 14(4), pp. 2327–2339. doi:10.1007/s12083-020-00944-z.

Niroshan Atimorathanna, D. et al. (2020) ‘NoFish; Total Anti-Phishing Protection System’, in 2020 2nd International Conference on Advancements in Computing (ICAC). 2020 2nd International Conference on Advancements in Computing (ICAC), pp. 470–475. doi:10.1109/ICAC51239.2020.9357145.

Nishikawa, H. et al. (2020) Analysis of Malicious Email Detection using Cialdini’s Principles, p. 142. doi:10.1109/AsiaJCIS50894.2020.00032.

Ortiz Garcés, I., Cazares, M.F. and Andrade, R.O. (2019) 'Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture', in 2019 International Conference on Computational Science and Computational Intelligence (CSCI). 2019 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 366–370. doi:10.1109/CSCI49370.2019.00071.

Ozcan, A. et al. (2021) 'A hybrid DNN–LSTM model for detecting phishing URLs', Neural Computing and Applications [Preprint]. doi:10.1007/s00521-021-06401-z.

Page, S. et al. (2019) 'Domain Classifier: Compromised Machines Versus Malicious Registrations', in, pp. 265–279. doi:10.1007/978-3-030-19274-7_20.

Paliath, S., Qbeitah, M.A. and Aldwairi, M. (2020) 'PhishOut: Effective Phishing Detection Using Selected Features', in 2020 27th International Conference on Telecommunications (ICT). 2020 27th International Conference on Telecommunications (ICT), pp. 1–5. doi:10.1109/ICT49546.2020.9239589.

Positive technologies. Top 10 most popular phishing topics in 2021 (2022). Available at: https://www.ptsecurity.com/ww-en/analytics/top-10-most-popular-phishing-topics-in-2021/ (Accessed: 26 April 2022).

Priestman, W. et al. (2019) 'Phishing in healthcare organizations: Threats, mitigation and approaches', BMJ health & care informatics, 26. doi:10.1136/bmjhci-2019-100031.

Priya, S., Selvakumar, S. and Velusamy, R.L. (2020) 'Gravitational Search-Based Feature Selection for Enhanced Phishing Websites Detection', in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 453–458. doi:10.1109/ICIMIA48430.2020.9074837.

Ramluckan, T., van Niekerk, B. and Martins, I. (2020) 'A change management perspective to implementing a cyber security culture', in. European Conference on Information Warfare and Security, ECCWS, pp. 442–448. doi:10.34190/EWS.20.059.

Ransomware Attacks Finnish Citizens Enrolled in Mental Healthcare - AskCyberSecurity.com (no date). Available at: https://www.askcybersecurity.com/ransomware-attacks-finnish-citizens-mental-healthcare/ (Accessed: 26 April 2022).

Ransomware attacks on US healthcare organizations cost $20.8bn in 2020' (2020) Comparitech, 11 February. Available at: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/ (Accessed: 26 April 2022).

Rao, R.S. and Pais, A.R. (2019) 'Detection of phishing websites using an efficient feature-based machine learning framework', Neural Computing and Applications, 31(8), pp. 3851–3873. doi:10.1007/s00521-017-3305-0.

Reuters (2016) 'Austria's FACC, hit by cyber fraud, fires CEO', 25 May. Available at: https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF (Accessed: 26 April 2022).

Roopak, S., Vijayaraghavan, A.P. and Thomas, T. (2019) 'On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection', in 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE). 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE), pp. 172–175. doi:10.1109/ICATIECE45860.2019.9063824.

S., E.R. and Ravi, R. (2020) 'A performance analysis of Software Defined Network-based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA)', Computer Communications, 153, pp. 375–381. doi:10.1016/j.comcom.2019.11.047.

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', Human behavior and emerging technologies, 3(5), pp. 854‐864. doi:10.1002/hbe2.301.

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

Sanders, E. B. N., and Stappers, P. J. (2014) 'Probes, toolkits, and prototypes: three approaches to making in codesigning', CoDesign. Taylor & Francis, pp. 5–14. doi: 10.1080/15710882.2014.888183

Sanders, E. B.-N. and Stappers, P. J. (2008) 'Co-creation and the new landscapes of design', CoDesign, 4(1), pp. 5–18. doi: 10.1080/15710880701875068.

Sanders, E.B.-N., Brandt, E. and Binder, T. (2010) 'A framework for organizing the tools and techniques of participatory design', in Proceedings of the 11th Biennial Participatory Design Conference on - PDC '10. the 11th Biennial Participatory Design Conference, Sydney, Australia: ACM Press, p. 195.

Shahriar, H. et al. (2019) 'Mobile anti-phishing: Approaches and challenges', Information Security Journal: A Global Perspective, 28(6), pp. 178–193. doi:10.1080/19393555.2019.1691293.

Shaik, I. et al. (2021) 'Privacy-Preserving Machine Learning for Malicious URL Detection', in, pp. 31–41. doi:10.1007/978-3-030-87101-7_4.

Sharton, B.R. (2021) 'Ransomware Attacks Are Spiking. Is Your Company Prepared?', Harvard Business Review, 20 May. Available at: https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared (Accessed: 26 April 2022).

Shedding Light on the DarkSide Ransomware Attack (2021) Security Intelligence, 10 May. Available at: https://securityintelligence.com/posts/darkside-oil-pipeline-ransomware-attack/ (Accessed: 26 April 2022).

Shukla, S. and Sharma, P. (2020) Detection of Phishing URL using Bayesian Optimized SVM Classifier, p. 1389. doi:10.1109/ICECA49313.2020.9297412.

Silveira, M. et al. (2021) Detection of Newly Registered Malicious Domains through Passive DNS, p. 3369. doi:10.1109/BigData52589.2021.9671348.

Singh, C., and Meenu (2020) Phishing Website Detection Based on Machine Learning: A Survey, p. 404. doi:10.1109/ICACCS48705.2020.9074400.

Sonowal, G. (2020a) 'Detecting Phishing SMS Based on Multiple Correlation Algorithms', SN Computer Science, 1(6), p. 361. doi:10.1007/s42979-020-00377-8.

Sonowal, G. (2020b) 'Phishing Email Detection Based on Binary Search Feature Selection', SN Computer Science, 1(4), p. 191. doi:10.1007/s42979-020-00194-z.

Sonowal, G. (2021) A Model for Detecting Sounds-alike Phishing Email Contents for Persons with Visual Impairments. doi:10.1109/econf51404.2020.9385451.

Sony hackers targeted employees with fake Apple ID emails | Computerworld (no date). Available at: https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html (Accessed: 26 April 2022).

Sornsuwit, P. and Jaiyen, S. (2019) 'A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting', Applied Artificial Intelligence, 33(5), pp. 462–482. doi:10.1080/08839514.2019.1582861.

Sreenidhi, A. et al. (2022) 'Detecting Phishing Websites Using Machine Learning', in, pp. 353–362. doi:10.1007/978-981-16-9873-6_32.

Steverson, K. et al. (2021) Cyber Intrusion Detection using Natural Language Processing on Windows Event Logs, p. 7. doi:10.1109/ICMCIS52405.2021.9486307.

Steves, M., Greene, K., and Theofanos, M. (2020) 'Categorizing human phishing difficulty: a Phish Scale', Journal of Cybersecurity, 6(1), p. tyaa009. doi:10.1093/cybsec/tyaa009.

Stoleru, G., Popescu, A. and Gavrilut, D. (2018) Increasing Protection Against Internet Attacks through Contextual Feature Pairing, p. 434. doi:10.1109/SYNASC.2018.00072.

Stop Ransomware | CISA (no date). Available at: https://www.cisa.gov/stopransomware (Accessed: 26 April 2022).

Subairu, S. et al. (2020) A Review of Detection Methodologies for Quick Response code Phishing Attacks, p. 5. doi:10.1109/ICCIS49240.2020.9257687.

Swedish Coop supermarkets shut due to US ransomware cyber-attack - BBC News (no date). Available at: https://www.bbc.com/news/technology-57707530 (Accessed: 26 April 2022).

Taha, A. (2021) 'Intelligent Ensemble Learning Approach for Phishing Website Detection Based on Weighted Soft Voting', Mathematics, 9. doi:10.3390/math9212799.

Tandale, K. and Pawar, S. (2020) Different Types of Phishing Attacks and Detection Techniques: A Review, p. 299. doi:10.1109/ICSIDEMPC49020.2020.9299624.

Tang, L. and Mahmoud, Q. (2021) 'A Deep Learning-Based Framework for Phishing Website Detection', IEEE Access, PP, pp. 1–1. doi:10.1109/ACCESS.2021.3137636.

Tchakounte, F. et al. (2018) 'A Game Theoretical Model for Anticipating Email Spear-Phishing Strategies', ICST Transactions on Scalable Information Systems, p. 166354. doi:10.4108/eai.26-5-2020.166354.

The Daily Swig. Washington residents' medical data exposed by a phishing attack on Spokane Regional Health District (2022) | Cybersecurity news and views. Available at: https://portswigger.net/daily-swig/washington-residents-medical-data-exposed-by-phishing-attack-on-spokane-regional-health-district (Accessed: 26 April 2022).

Touro College Illinois. The 10 Biggest Ransomware Attacks of 2021 (2021). Available at: https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php (Accessed: 26 April 2022).

Trend Micro. Ransomware - Definition (2022). Available at: https://www.trendmicro.com/vinfo/us/security/definition/ransomware (Accessed: 26 April 2022).

Triple-Digit Increase in Cyberattacks | Accenture (2021) WordPressBlog. Available at: https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks (Accessed: 26 April 2022).

Ulqinaku, E., Lain, D. and Capkun, S. (2019) 2FA-PP: 2nd-factor phishing prevention, p. 70. doi:10.1145/3317549.3323404.

UX Magazine, (2012). Creativity-based Research: The Process of Co-Designing with Users. Available at: https://uxmag.com/articles/creativity-based-research-the-process-of-co-designing-with-users (Accessed: 28 April 2022).

Vaishnavi, D. et al. (2021) 'A Comparative Analysis of Machine Learning Algorithms on Malicious URL Prediction', in 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1398–1402. doi:10.1109/ICICCS51141.2021.9432138.

Valentim, R. et al. (2021) 'Augmenting phishing squatting detection with GANs', in Proceedings of the CoNEXT Student Workshop. CoNEXT '21: The 17th International Conference on emerging Networking EXperiments and Technologies, Virtual Event Germany: ACM, pp. 3–4. doi:10.1145/3488658.3493787.

Vaughn, L.M. and Jacquez, F. (2020) 'Participatory Research Methods – Choice Points in the Research Process', Journal of Participatory Research Methods, 1(1), p. 13244. doi:10.35844/001c.13244.

Venkatesha, S., Reddy, K.R. and Chandavarkar, B.R. (2021) 'Social Engineering Attacks During the COVID-19 Pandemic', SN Computer Science, 2(2), p. 78. doi:10.1007/s42979-020-00443-1.

Wahsheh, H.A.M., and Al-Zahrani, M.S. (2021) 'Secure Real-Time Computational Intelligence System Against Malicious QR Code Links', INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, 16(3). Available at: http://univagora.ro/jour/index.php/ijccc/article/view/4186 (Accessed: 5 March 2022).

Wang, Y. and Duncan, I. (2019) 'A Novel Method to Prevent Phishing by using OCR Technology', in 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2019 International Conference on Cyber Security

and Protection of Digital Services (Cyber Security), Oxford, United Kingdom: IEEE, pp. 1–5. doi:10.1109/CyberSecPODS.2019.8885101.

Wash, R. (2020) 'How Experts Detect Phishing Scam Emails', Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), pp. 1–28. doi:10.1145/3415231.

Wen, Z. et al. (2019) What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, p. 12. doi:10.1145/3290605.3300338.

What is a cyber attack? | IBM (no date). Available at: https://www.ibm.com/topics/cyber-attack (Accessed: 26 April 2022).

Wu, J. et al. (2019) Convolutional Neural Network with Character Embeddings for Malicious Web Request Detection, p. 627. doi:10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00094.

Xuan, C.D., Dinh, H. and Victor, T. (2020) 'Malicious URL Detection based on Machine Learning', International Journal of Advanced Computer Science and Applications, 11(1). doi:10.14569/IJACSA.2020.0110119.

Yang, K. and Su, S. (2019) Secure Email Login Based on Lightweight Asymmetric Identities, p. 29. doi:10.1145/3371676.3371683.

Younis, A. and Musbah, M. (2020) A Framework to Protect Against Phishing Attacks. doi:10.1145/3410352.3410825.

Zhou, Z. et al. (2020) 'Tear Off Your Disguise: Phishing Website Detection Using Visual and Network Identities', in, pp. 763–780. doi:10.1007/978-3-030-41579-2_44.

Zhu, H. (2020) 'Online meta-learning firewall to prevent phishing attacks', Neural Computing and Applications, 32(23), pp. 17137–17147. doi:10.1007/s00521-020-05041-z.

Appendix 1. The empirical data from articles

Name of the publication	Classification	Targeted Phishing vector	The underlying methodology of the solution	Target area
Finding Phish in a Haystack: A Pipeline for Phishing Classification on Certificate Transparency Logs	Approach	Website	Machine Learning	Generic
A Framework to Protect Against Phishing Attacks	Framework	Generic	Gamification	End users
A Phishing Mitigation Solution Using Human Behaviour and Emotions That Influence the Success of Phishing Attacks	Approach	Generic	Machine Learning	Organizations
Following Passive DNS Traces to Detect Stealthy Malicious Domains Via Graph Inference	Scheme	Website	Machine Learning	Generic
Human Risk Factors in Cybersecurity	Recommendations	E-mail	Knowledge transfer	End users
A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection	Method	Generic	Machine Learning	Generic
Click This, Not That: Extending Web Authentication with Deception	System	E-mail	Hardware	Organizations
PhAttApp: A Phishing Attack Detection Application	Solution	E-mail	Knowledge transfer	End users
Secure Email Login Based on Lightweight Asymmetric Identities	Solution	E-mail	Cryptography	End users
A Flexible Phishing Detection Approach Based on Software-Defined Networking Using Ensemble Learning Method	Approach	Website	Programming	End users
Detecting Telephone-Based Social Engineering Attacks Using Scam Signatures	Approach	Vishing	Machine Learning	Generic
How Experts Detect Phishing Scam Emails	Recommendations	E-mail	Knowledge transfer	Organizations
Detecting Spam Tweets Using Machine Learning and Effective Preprocessing	Approach	Social Network	Machine Learning	End users
Augmenting Phishing Squatting Detection with GANs	Solution	Website	Machine Learning	Generic
Visualizing and Interpreting RNN Models in URL-Based Phishing Detection	Model	Website	Neural network	Generic
Avoid Phishing Traps	Recommendations	Generic	Knowledge transfer	Organizations
A Design of an Anti-Phishing Training System Collaborated with Multiple Organizations	System	E-mail	Hardware	Organizations
LinkMan: Hyperlink-Driven Misbehavior Detection in Online Security Forums	Approach	Social Network	Machine Learning	Generic

URL-Based Phishing Detection Using the Entropy of Non-Alphanumeric Characters	Framework	Website	NonAlphanumeric Characters	Generic
What. Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game	Framework	E-mail	Gamification	End users
PhishLedger: A Decentralized Phishing Data Sharing Mechanism	Solution	Generic	Blockchain	Organizations
Machine Learning for Tree Structures in Fake Site Detection	Method	Website	Machine Learning	Generic
2FA-PP: 2nd Factor Phishing Prevention	Tool	Website	Hardware	End users
A hybrid DNN–LSTM model for detecting phishing URLs	Model	Website	Machine Learning	End users
A robust intelligent zero-day cyber-attack detection technique	Model	Devices	Machine Learning	Admin
Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender on Thai Employees Associated with Phishing Attack	Approach	E-mail	Knowledge transfer	End users
Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks	Recommendations	Generic	Generic	Generic
Detecting Phishing SMS Based on Multiple Correlation Algorithms	Model	Smishing	Machine Learning	Generic
Don't click: towards an effective anti-phishing training. A comparative literature review	Recommendations	Generic	Knowledge transfer	End users
DSmishSMS-A System to Detect Smishing SMS	System	Smishing	Machine Learning	Generic
PenQuest: a gamified attacker/defender meta-model for cyber security assessment and education	Model	Generic	Gamification	End users
Phishing Email Detection Based on Binary Search Feature Selection	Method	E-mail	Machine Learning	End users
Social Engineering Attacks During the COVID-19 Pandemic	Guidelines	Generic	Generic	Generic
The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review	Recommendations	Generic	Generic	Generic
Warning users about cyber threats through sounds	Tool	Website	Human-centric	End users
A Case Study of Phishing Incident Response in an Educational Organization	Guidelines	E-mail	Knowledge transfer	End users
A Change Management Perspective on Implementing a Cyber Security Culture	Framework	Generic	Knowledge transfer	Organizations

A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea	Framework	Vishing	Human-centric	Generic
A review of phishing attacks and countermeasures for the internet of things-based smart business applications in industry 4.0	Guidelines	Generic	Generic	End users
Alerting Users About Phishing Attacks	Recommendations	Website	Knowledge transfer	End users
Deep Neural Network Based Phishing Classification on a High-Risk URL Dataset	Approach	Website	Neural Network	Generic
Detection of phishing attacks with machine learning techniques in cognitive security architecture	Method	Website	Machine Learning	Generic
Development of anti-phishing browser based on random forest and rule of extraction framework	Tool	Website	Machine Learning	End users
Informing, simulating experience, or both: A field experiment on phishing risks	Approach	Generic	Generic	End users
Machine learning classification algorithms for adware in android devices: A comparative evaluation and analysis	Method	Website	Machine Learning	Generic
Preventing and Mitigating Ransomware: A Systematic Literature Review	Recommendations	Generic	Generic	Generic
Victim or Attacker? A Multi-dataset Domain Classification of Phishing Attacks	Method	Website	Machine Learning	Generic
A Comparative Analysis of Machine Learning Algorithms on Malicious URL Prediction	Method	Website	Machine Learning	End users
A Comprehensive Survey on Identification and Analysis of Phishing Website based on Machine Learning Methods	Method	Website	Machine Learning	Generic
A Deep Learning-Based Framework for Phishing Website Detection	Framework	Website	Neural network	End users
A Hybrid Security Solution for Mitigating Cyber-Attacks on Info-Communication Systems	Solution	WiFi	Cryptography	Organizations
A Model for Detecting Sounds-alike Phishing Email Contents for Persons with Visual Impairments	Model	Website	Machine Learning	End users
A New Email Phishing Training Website	System	E-mail	Gamification	Organizations
A Novel Method to Prevent Phishing by using OCR Technology	Approach	Website	Programming	End users
A Review of Detection Methodologies for Quick Response code Phishing Attacks	Method	QR code	Generic	Generic

An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage	System	Website	pseudonymisation technique	End users
An Intelligent System for Phishing Attack Detection and Prevention	System	Website	Machine Learning	End users
Analysis of Malicious Email Detection using Cialdini's Principles	Approach	E-mail	Machine Learning	Generic
Anti-phishing System using LSTM and CNN	System	Website	Neural network	Generic
Computer Vision-Based Framework For Detecting Phishing Webpages	Framework	Website	Machine Learning	End users
Convolutional Neural Network with Character Embeddings for Malicious Web Request Detection	Approach	Website	Machine Learning	Generic
Cyber Intrusion Detection using Natural Language Processing on Windows Event Logs	Approach	Website	Machine Learning	End users
Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection	Solution	Website	Neural network	End users
Detecting Phishing Websites Using Machine Learning	System	Website	Hardware	Admin
Detection of Newly Registered Malicious Domains through Passive DNS	Approach	Website	Machine Learning	Generic
Detection of Phishing URL using Bayesian Optimized SVM Classifier	Method	Website	Machine Learning	Generic
Detection of Phishing Websites by Using Machine Learning-Based URL Analysis	Approach	Website	Machine Learning	Generic
Different Types of Phishing Attacks and Detection Techniques: A Review	Recommendations	Website	Generic	End users
EDITH - A Robust Framework for Prevention of Cyber Attacks in the Covid Era	Framework	Website	Generic	Generic
Email Anti-Phishing Detection Application	System	Website	Hardware	End users
Generating Rules to Detect Phishing Websites Using URL Features	Approach	Website	Data mining	Generic
Gravitational Search-Based Feature Selection for Enhanced Phishing Websites Detection	Approach	Website	Machine Learning	Generic
Heuristic Phishing Detection and URL Checking Methodology Based on Scraping and Web Crawling	Method	E-mail	Programming	Generic
Intelligent Phishing Url Detection: A Solution Based On Deep Learning Framework	Approach	Website	Neural network	Generic
Machine Learning Classification Algorithms for Phishing Detection: A Comparative Appraisal and Analysis	Model	Generic	Machine Learning	Generic

Machine Learning Detection for SMiShing Frauds	Tool	Smishing	Machine Learning	End users
Mitigating Email Phishing Attacks using Convolutional Neural Networks	Framework	E-mail	Neural network	Generic
Naive and Neighbour Approach to Phishing Detection	Approach	Website	Machine Learning	Generic
NoFish; Total Anti-Phishing Protection System	System	E-mail	Machine Learning	Generic
On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection	Method	Website	Machine Learning	Generic
PhishFry - A Proactive Approach to Classify Phishing Sites Using SCIKIT Learn	Tool	Website	Machine Learning	Generic
PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System	System	Website	Machine Learning	Generic
Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process	Recommendations	Generic	Knowledge transfer	End users
Phishing URL Classification Analysis Using ANN Algorithm	Model	Website	Machine Learning	Generic
Phishing URL Detection via CNN and Attention-Based Hierarchical RNN	Approach	Website	Neural network	Generic
Phishing Website Classification and Detection Using Machine Learning	Method	Website	Machine Learning	Generic
Phishing Website Detection Based on Machine Learning: A Survey	Method	Generic	Generic	Generic
PhishOut: Effective Phishing Detection Using Selected Features	Approach	Website	Machine Learning	Generic
Preventive Techniques of Phishing Attacks in Networks	Recommendations	Generic	Generic	Generic
PunyVis: A Visual Analytics Approach for Identifying Homograph Phishing Attacks	System	Wifi	Machine Learning	Generic
Quick Response Code Validation and Phishing Detection Tool	Tool	QR code	Data mining	End users
Secure Suite: An Open-Source Service for Internet Security	System	Website	Hardware	Generic
Social Engineering and the Dangers of Phishing	Recommendations	Generic	Knowledge transfer	End users
SpoofCatch: A Client-Side Protection Tool Against Phishing Attacks	Tool	Website	Machine Learning	Generic
Towards the Detection of Phishing Attacks	Approach	Website	Programming	Generic
Trust me and Click! A Pilot Study of Cognitive Walkthrough for Phishing Emails	Method	E-mail	Human-centric	End users
Verbal Deception Cue Training for the Detection of Phishing Emails	Recommendations	E-mail	Knowledge transfer	Generic

WC-PAD: Web Crawling based Phishing Attack Detection	Tool	Website	Human-centric	Generic
Zero-Day attack prevention Email Filter using Advanced Machine Learning	Approach	E-mail	Machine Learning	Generic
A Game Theoretical Model for Anticipating Email Spear-Phishing Strategies	Model	E-mail	Gamification	Organizations
A HYBRID PHISHING DETECTION APPROACH FOR MOBILE APPLICATION	Approach	Website	Machine Learning	End users
A machine learning-based approach for phishing detection using hyperlinks information	Approach	Website	Machine Learning	Generic
A Mamdani Type Fuzzy Inference System to Calculate Employee Susceptibility to Phishing Attacks	System	Generic	Fuzzy logic	Organizations
A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting	Model	Generic	Machine Learning	Generic
A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA)	Framework	Generic	Neural network	Generic
Adopting automated whitelist approach for detecting phishing attacks	Approach	Website	Programming	Admin
Agenda Pushing in Email to Thwart Phishing	System	E-mail	Programming	End users
AI@ntiPhish - Machine Learning Mechanisms for Cyber-Phishing Attack	Approach	Website	Human-centric	Generic
An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL	Model	Website	Neural network	Generic
An effective security alert mechanism for real-time phishing tweet detection on Twitter	Model	Social Network	Machine Learning	End users
Analyzing and eliminating phishing threats in IoT, network, and other Web applications using iterative intersection	Approach	Website	Programming	End users
Automatic detection of phishing pages with event-based request processing, deep-hybrid feature extraction, and light gradient boosted machine model	Framework	Website	Machine Learning	Generic
Browser Extension based Hybrid Anti-Phishing Framework using Feature Selection	Framework	Website	Machine Learning	Generic
Catching the Phish: Detecting Phishing Attacks Using Recurrent Neural Networks (RNNs)	System	E-mail	Machine Learning	Generic
Categorizing human phishing difficulty: a Phish Scale	Tool	E-mail	Knowledge transfer	Organizations
Detecting E-Banking Phishing Website using C4.5 Algorithm	Method	Website	Data mining	End users
Detecting Internet of Things attacks using distributed deep learning	Framework	Devices	Machine Learning	End users

Detecting phishing attacks using a combined model of LSTM and CNN	Approach	Website	Machine Learning	Generic
Detection of Phishing in Internet of Things Using Machine Learning Approach	Model	Devices	Machine Learning	Generic
Detection of phishing websites using an efficient feature-based machine learning framework	System	Website	Machine Learning	Generic
Detection Technique and Mitigation Against a Phishing Attack	Method	Website	Programming	Admin
Domain Classifier: Compromised Machines Versus Malicious Registrations	Method	Website	Machine Learning	Generic
Don't Forget the Human: a Crowdsourced Approach to Automate Response and Containment Against Spear Phishing Attacks	Model	Generic	Knowledge transfer	End users
Enterprise Credential Spear-phishing attack detection	System	E-mail	Programming	Organizations
HinPhish: An Effective Phishing Detection Approach Based on Heterogeneous Information Networks	Approach	Website	Machine Learning	Generic
Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach	Approach	Devices	Knowledge transfer	Generic
Improving Phishing Awareness in the United States Department of Defense	Approach	Generic	Knowledge transfer	Organizations
Increasing Protection against Internet Attacks through Contextual Feature Pairing	Approach	Website	Machine Learning	Generic
Intelligent Association Classification Technique for Phishing Website Detection	Model	Website	Machine Learning	Generic
Intelligent Ensemble Learning Approach for Phishing Website Detection Based on Weighted Soft Voting	Approach	Website	Machine Learning	End users
Intelligent phishing detection scheme using deep learning algorithms	System	Website	Machine Learning	Generic
Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text	Scheme	Generic	Fuzzy logic	Generic
LogoSENSE: A companion HOG based logo detection scheme for phishing web page and E-mail brand recognition	System	Website	Machine Learning	End users
Machine Learning-Based Malicious X.509 Certificates' Detection	System	Website	Machine Learning	Generic
Malicious URL Detection based on Machine Learning	Method	Website	Machine Learning	Generic
Mobile anti-phishing: Approaches and challenges	Approach	Mobile application	Generic	Generic

New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing	Scheme	Mobile application	Cryptography	Generic
On detecting and mitigating phishing attacks through featureless machine learning techniques	System	Website	Machine Learning	Generic
Online meta-learning firewall to prevent phishing attacks	Tool	Generic	Machine Learning	Generic
Phishing Email Detection based on Named Entity Recognition	Method	E-mail	Machine Learning	Generic
Phishing in Depth - Modern Methods of Detection and Risk Mitigation	Scheme	E-mail	Knowledge transfer	Organizations
Phishing in healthcare organisations: threats, mitigation and approaches	Recommendations	Generic	Knowledge transfer	Organizations
Phishing page detection via learning classifiers from page layout feature	Approach	Generic	Machine Learning	Generic
Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning	Framework	Website	Neural network	Generic
Phishing Website Detection: Forest by Penalizing Attributes Algorithm and Its Enhanced Variations	Model	Website	Machine Learning	Generic
Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages	System	Website	Neural network	Generic
Privacy Preserving Machine Learning for Malicious URL Detection	Approach	Website	Machine Learning	Generic
Privacy-aware detection framework to mitigate new-age phishing attacks	Framework	Website	Knowledge transfer	End users
Proactive Detection of Phishing Kit Traffic	Model	E-mail	Neural Network	Admin
Ransomware: Recent advances, analysis, challenges and future research directions	Recommendations	Generic	Generic	Generic
Rotation Forest-Based Logistic Model Tree for Website Phishing Detection	Model	Generic	Machine Learning	Generic
Secure Real-Time Computational Intelligence System Against Malicious QR Code Links	Method	QR code	Machine Learning	Generic
Social Engineering Attacks: Recent Advances and Challenges	Guidelines	Generic	Generic	Generic
Tear Off Your Disguise: Phishing Website Detection Using Visual and Network Identities	Approach	Website	Machine Learning	Organizations
Towards benchmark datasets for machine learning based website phishing detection: An experimental study	Guidelines	Website	Machine Learning	Generic

Unified Payment Interface (UPI) platform: Conniving tool for Social Engineering Attack	Recommendations	Generic	Knowledge transfer	Generic
VPCID-A VoIP Phone Call Identification Database	Database	Vishing	Machine Learning	Generic
Browser Extension based Hybrid Anti-Phishing Framework using Feature Selection	Framework	Website	Machine Learning	Generic