Strategy Selection Against Cyber and Phishing Attacks in the Financial Sector Using MCDM Methods

Araştırma Makalesi/Research Article

Rafetcan ÖZGÜR[1], Tamer EREN[1]*

[1]Dept. of Industrial Engineering, Kirikkale University, Kırıkkale, TÜRKİYE

rafetcanozgur@gmail.com, teren@kku.edu.tr

(Geliş/Received:21.06.2025; Kabul/Accepted:30.03.2026)

DOI: 10.17671/gazibtd.1724633

***Abstract*—** The financial sector constitutes a prime target for cyber attackers owing to its high volume of transactions and the sensitive nature of its data. The most critical cyber-attacks pertinent to this sector have been identified, with the most prevalent type, the phishing attack, being examined in detail. Phishing attacks, in particular, can lead to severe data breaches and financial losses at both individual and institutional levels. In this context, the selection of the appropriate security strategy to prioritize against this type of attack is of paramount importance. Following expert consultation, six criteria were established and subsequently prioritized: effectiveness, cost, implementation difficulty, sustainability, user acceptance, and scope. Consequently, a priority ranking was assigned to various strategies, including Employee Training, E-mail Filtering Systems, Multi-Factor Authentication (MFA), Zero Trust Architecture, Segregation of Duties, DNS Filtering and Web Security, and Endpoint Security. The criteria weights used to establish this priority ranking were derived using Multi-Criteria Decision-Making (MCDM) methods, namely Pythagorean Fuzzy AHP (PFAHP) and Neutrosophic Fuzzy AHP (NFAHP). The final prioritized strategy or strategies were then determined using the TOPSIS and PROMETHEE methods.

***Keywords*—** cyber security, financial sector, phishing, multi-criteria decision-making, PFAHP, NFAHP, TOPSIS, PROMETHEE

ÇKKV Yöntemleri Kullanılarak Finans Sektöründe Siber ve Oltalama Saldırılarına Karşı Strateji Seçimi

***Özet*—** Finans sektörü, yüksek işlem hacmi ve hassas veri yapısı nedeniyle siber saldırganlar için öncelikli hedefler arasında yer almaktadır. Bu sektör için en kritik siber saldırılar belirlenmiş ve aralarından en sık karşılaşılan tür olan kimlik avı saldırısı detaylıca incelenmiştir. Özellikle kimlik avı saldırıları, hem bireysel hem kurumsal düzeyde ciddi veri ihlallerine ve finansal kayıplara yol açabilmektedir. Bu bağlamda, bu saldırı türüne yönelik öncelik verilecek doğru güvenlik stratejisinin seçimi son derece büyük bir önem taşımaktadır. Uzman görüşleri sonucunda Etkililik, maliyet, uygulama zorluğu, sürdürülebilirlik, kullanıcı kabulü ve kapsam olmak üzere altı kriter belirlenmiş ve belirlenen kriterler önceliklendirilmiştir. Strateji olarak ise Çalışan Eğitimi, E-posta Filtreleme Sistemleri, Çok Faktörlü Kimlik Doğrulama (MFA), Zero Trust, Görev Ayrımı, DNS Filtreleme ve Web Güvenliği ve Uç Nokta Güvenliği gibi stratejiler için öncelik sıralaması verilmiştir. Öncelik sıralamasının belirlenmesinde kullanılan kriter ağırlıkları çok kriterli karar verme (ÇKKV) yöntemlerinden olan Pisagor Bulanık AHP (PBAHP) ve Nötrosofik Bulanık AHP (NBAHP) kullanılarak sağlanmış, TOPSIS ve PROMETHEE yöntemleri ile de öncelik verilmesi gereken strateji(-ler) belirlenmiştir.

***Anahtar Kelimeler*—** siber güvenlik, finans sektörü, kimlik avı, çok kriterli karar verme, PBAHP, NBAHP, TOPSIS, PROMETHEE

1. INTRODUCTION

Influenced by digitalization, the financial sector is currently undergoing a rapid digital transformation. Numerous financial institutions operate within the financial market, among which banks hold a significant position [1]. Banking operations, payment systems, investment services, and customer interactions have largely migrated to digital platforms, a shift that has both facilitated service delivery and increased customer accessibility [2]. However, these developments have also introduced significant security risks. Cyber-attacks constitute a serious threat to this sector, particularly due to the direct targeting of financial data [3]. At the forefront of these threats are phishing attacks. The most concrete example of this attack type is the "Carbanak" operation, which began in late 2013. In this operation, criminals infiltrated the systems of over 100 banks, stealing approximately 1 billion dollars and demonstrating how such an attack could escalate into a major heist [4-6].

Phishing attacks are a type of cyber-attack, typically conducted via email, SMS, or fraudulent websites, aimed at acquiring personal or corporate information by deceiving individuals or institutional employees. These attacks target not only individual users but also corporate structures, potentially leading to large-scale data breaches and financial losses. Numerous cybersecurity threats, such as the acquisition of personal data using malicious software, the disclosure of confidential information belonging to institutions or governments, and the disabling of services for commercial companies, are among the dangers present in cyberspace [7]. In particular, banks, insurance companies, investment firms, and financial technology (fintech) companies stand out as high-yield targets for attackers. Failure to take necessary precautions can result in not only monetary damages but also loss of corporate reputation, legal liabilities, and a severe erosion of customer trust. The effective prevention of phishing attacks is not achievable solely through the implementation of technical security measures. The human factor plays a key role in the success of these attacks; therefore, it is necessary to raise awareness levels, restructure processes, and establish defense mechanisms through a strategic approach [8].

In the literature, the problem of strategy selection is addressed as a multi-criteria decision-making (MCDM) problem because it necessitates the evaluation of numerous alternatives and varying priorities. It is observed that these aforementioned methods are preferred for subjects of importance to the financial sector, such as performance management, strategy selection, and the analysis of investment alternatives [9]. When dealing with complex threats like phishing attacks, decision-makers must consider multiple and often conflicting criteria. For instance, a strategy may be highly effective, yet its implementation cost or sustainability could be weak. Therefore, decisions must be made not only through intuitive approaches but also with systematic and analytical methods [10].

Techniques used in the literature include methods such as Analytic Hierarchy Process (AHP), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), Elimination and Choice Expressing Reality (ELECTRE), Preference Ranking Organization Method for Enrichment of Evaluations (PROMETHEE), Multicriteria Optimization and Compromise Solution (VIKOR), Analytic Network Process (ANP) and fuzzy logic. These methods enable the weighting of different criteria and the ranking of alternatives according to these criteria. Thus, decision-makers can determine the most suitable strategy by considering both subjective and objective data. At this point, it becomes imperative for financial institutions to conduct a multi-dimensional evaluation when choosing among different strategic options. The fact that strategy selection is not only a technical but also a managerial and operational decision makes the issue even more complex [11]. MCDM methods are widely used in solving such problems [11-12].

Many factors, such as effectiveness, sustainability, risk mitigation, ease of implementation, adaptability, and speed of intervention, are among the important elements to be considered in this selection process. This study aims to select the most critical strategy by taking these criteria into account.

The plan of the study is as follows: The second section describes cyber-attacks in the financial sector and explains applicable approaches. The third section of the study addresses MCDM approaches and explains the structure of the methods used. In the fourth section, the impacts of phishing attacks on the financial sector are examined, and a literature review on the subject is conducted. The fifth section presents in detail the implementation steps carried out according to the determined criteria and alternatives. In the sixth and final section, the results obtained from the study are evaluated, and recommendations for future research are provided.

2. CYBER ATTACKS IN THE FINANCIAL SECTOR

Rapid advancements in digital technologies, while facilitating access to information, also bring with them significant information security risks [13]. This situation has substantially increased the threats faced by both individuals and institutions in digital environments, making the issue of ensuring information security a primary agenda item for organizations. Cybersecurity aims to protect the confidentiality, integrity, and availability of information and communication systems. As the scope of measures taken at the corporate level expands, the importance of investments and strategic decisions in this area also increases. Due to the potentially devastating impacts of security breaches on a business, cybersecurity is identified as one of the greatest risks for contemporary organizations [14]. In this context, cybersecurity has transcended being merely a technical discipline and has transformed into a strategic issue that directly affects the sustainability and competitive advantage of institutions. This transformation is most evident specifically within the

financial sector. As a requirement of business models, laws, standards, and regulations, the implementation of information technology security measures and the auditing of these processes emerge as a vital function in the banking sector [15]. The banking and financial services sector has become highly dependent on digital systems in terms of transaction volume, number of users, and the amount of data it holds. Should the security of these systems be compromised, serious consequences can arise not only in terms of financial losses but also regarding customer trust, brand reputation, and legal liabilities. A significant portion of large-scale cyber-attacks occurring globally has targeted the financial sector. Some of the types of attacks directed at the financial sector include the following:

- **Phishing and Targeted Spear Phishing:** Through fraudulent emails or messages, the credentials of employees or customers are stolen. Phishing is the most common method used by cyber attackers to gain access to a financial institution's network [16]. In 2014, a bank in the United States was hacked, resulting in the compromise of more than 80 million user accounts [17].
- **Ransomware Attacks:** This is an attack method wherein access to the computers or data of institutional personnel is blocked, and a ransom is demanded to restore system functionality [16]. The WannaCry ransomware attack, which occurred in 2017 and was considered the worst of its kind to date, had impactful and devastating consequences [18].
- **DDoS Attacks:** The aim is to cause service interruptions by directing an excessive amount of traffic to online financial platforms, such as banks or stock exchanges. These attacks are typically used to support ransom demands or to conceal another attack. In their study, Abhishta et al. (2020) examined 27 different incidents from the year 2016 [19].
- **Insider Threats:** This refers to the situation where individuals working in financial institutions, either consciously or unconsciously, collaborate with cyber attackers to leak data or provide unauthorized access to systems. This type of threat is of critical importance, especially concerning employees who have broad access privileges. As an example, it was alleged that in 2019, more than 100 million customer records at a bank in the United States were stolen by a single individual [20].
- **Advanced Persistent Threats:** These are advanced types of cyber-attacks, often state-sponsored, that can remain undetected on a target system for an extended period. These attacks are carried out for the purpose of data exfiltration or acquiring financial intelligence. The Stuxnet APT software, discovered in 2010 and developed by the United States and Israel, was an attack carried out with the aim of causing physical damage to the centrifuges in Iran's nuclear facilities [21].
- **Man-in-the-Middle Attacks:** This involves intercepting the data transmission between a user and a financial service provider to monitor or manipulate the communication. Session hijacking on public Wi-Fi networks is a typical example of this type of attack [22].
- **SQL Injection and Web Vulnerabilities:** This is the act of gaining unauthorized access to databases by injecting malicious commands into web applications that have weak input validation systems. In 2015, the British company TalkTalk suffered a loss of 77 million pounds due to an attack that exploited an SQL Injection vulnerability [23].
- **Credential Stuffing:** This is an attempt to gain unauthorized access by automatically testing username and password combinations, obtained from different platforms, on financial systems. In 2019, the company Dunkin' Donuts was subjected to a credential stuffing attack. In the attack, the attackers gained access to numerous customer accounts [24].
- **Supply Chain Attacks:** This is the infiltration of a system through third-party software and service providers used by financial institutions. The SolarWinds attack is the most prominent example of this type of attack. It targeted approximately 18,000 government and commercial organizations, including many prominent institutions, giving attackers access to top-secret government information [25].
- **Social Engineering:** The objective is to acquire users' personal or financial data through phone calls or text messages. Fraudulent verification requests and account update notifications are among the common tactics used. The 2020 Twitter attack targeted approximately 130 high-profile accounts, including those of U.S. politicians and industry leaders [26].
- **Zero-Day Vulnerabilities:** These are attacks carried out by exploiting software vulnerabilities that are not yet known to the vendor or users. Such vulnerabilities are typically high-impact and fast-spreading threats. In the Stuxnet APT software attack, also mentioned in the Advanced Persistent Threats section, four different zero-day vulnerabilities were used to facilitate system infiltration and increase the malware's impact [27].
- **Business Email Compromise:** Fraudulent money transfer requests are made from accounting or finance personnel via emails that impersonate senior executives. CEO fraud is a typical example of this method. In their study, Papathanasiou et al. (2023) provided prominent examples of BEC attacks. The study summarized data such as the incidents, the year they occurred, and the details of what transpired [28].
- **ATM and Card Skimming:** The objective is to copy user card data via skimming devices or fraudulent card readers placed on bank ATMs. Additionally, data leakage can occur through malicious software placed on digital payment pages. ATM card skimming devices were discovered at grocery stores in York and Lancaster

County, and in Philadelphia, some benefits were stolen using similar devices [29].

- **Fileless Malware:** Persistence in systems is achieved through software that executes malicious activities in memory without leaving a trace on the disk. In their study, Lee et al. (2021) analyzed 10 fileless cyber attacks that have emerged in recent years [30].
- **API Vulnerabilities:** Interfaces used in financial services can become vulnerable to threats such as unauthorized access, data leakage, and transaction manipulation when adequate security measures are not taken. Between 2013 and 2015, the company Cambridge Analytica illicitly collected the private data of 87 million users through a Facebook API vulnerability for the purpose of creating personality profiles to be used in political campaigns. This breach resulted in Facebook being fined 5 billion dollars and the bankruptcy of Cambridge Analytica [31].
- **SIM Swapping:** A phone number is transferred to a SIM card under the control of a cyber attacker. With this method, SMS-based two-factor authentication systems can be bypassed, and access to accounts can be gained. In 2019, the phone number of then-Twitter CEO Jack Dorsey was compromised in a SIM Swap attack, and racist and offensive messages were subsequently posted from his account. [32].
- **Deepfake:** This involves attempting to create financial instructions by impersonating senior executives through fraudulent audio and video recordings produced using artificial intelligence technologies. The CEO of a UK-based energy firm was deceived over the phone by a deepfake voice that used AI to mimic the company's German executive, leading him to urgently transfer $234,000 to a supplier [33].
- **Misuse of Cloud Services:** The leakage of critical data or the gaining of unauthorized access through improperly configured cloud services poses a growing security risk for financial institutions [34].
- **Mobile Banking Trojans:** The objective is to gain access to financial data on mobile devices through certain types of malicious software. This type of malware is typically spread through fraudulent applications. As of August 2019, a virus named Agent Smith had infected approximately 22,000 devices across Ukraine, modifying their Android application codes [35].
- **SWIFT Network Attacks:** Large money transfers are conducted by creating fraudulent transaction instructions directed at the SWIFT system, which is used for international fund transfers. These attacks require a high degree of coordination and technical expertise. In the 2016 Bangladesh Bank heist, attackers attempted to transfer nearly 1 billion dollars to accounts in several countries by sending fraudulent instructions through the bank's SWIFT system, resulting in a loss of 81 million dollars [36].

The attacks described generally focus on the vulnerabilities of corporate networks and systems. In recent years, it has been observed that user-focused attacks, particularly phishing attacks, have become prominent. Phishing attacks can inflict damage on banks and customers vulnerable to such security threats [37]. This type of attack is highly attractive to cyber attackers because it can succeed through user behavior without targeting technically complex systems, and, when successful, it provides direct access to critical data such as login credentials, credit card numbers, or digital sessions. Phishing attacks can result in the compromise not only of individuals but also of companies and even national security [38]. If an employee's credentials are compromised, attackers can gain access to that employee's computer, thereby accessing both the company's internal systems and customer data, which can lead to a large-scale data breach.

There are numerous variables that banks and other financial institutions must consider when formulating their cybersecurity strategies. A wide spectrum of alternative solutions must be evaluated, ranging from traditional antivirus software to advanced threat detection systems, and from employee awareness training to multi-factor authentication applications. However, the effectiveness, cost, feasibility, and sustainability of each solution differ. Strategy selection, by its nature, is a multi-criteria decision problem.

In this respect, the cybersecurity strategy selection process is not merely a technical evaluation; it is also a multi-dimensional, strategic decision-making process aligned with corporate objectives. Especially in an environment where social engineering-based attacks like phishing are prevalent, creating comprehensive and balanced security policies that incorporate the human factor has become a necessity. Phishing, ransomware, and other cyber threats can jeopardize customer data and the digital infrastructures of banks. Banks must strengthen their cybersecurity strategies and be continuously prepared for new threats [39].

The problem addressed in this study is based on the necessity for an organization operating in the financial sector to select the most suitable cybersecurity strategy against phishing attacks. This selection process takes place in a decision-making environment where multiple strategic alternatives and numerous decision criteria exist. Therefore, this problem is suitable for the application of MCDM methods.

3. METHODS

As decision-making processes become increasingly complex in the contemporary world, MCDM methods have become one of the most frequently utilized analysis tools across various disciplines. Especially in environments of uncertainty, where numerous alternatives and various criteria for evaluating them exist, it becomes quite difficult for decision-makers to reach sound conclusions using only intuitive methods. In such situations, MCDM approaches,

which systematize the decision process and address different criteria in a structured manner, come to the forefront. MCDM methods are encountered in situations where a selection must be made from a set of alternatives or candidates based on a series of criteria or attributes [40]. Consequently, it becomes necessary to consider numerous criteria to select the most suitable option from among the alternatives. This, in turn, directs decision-makers toward methods that allow them to evaluate alternatives systematically.

When selecting from alternatives, decision-makers must consider multiple criteria to find the option that most effectively achieves conflicting objectives [41]. Indeed, the criteria involved in a decision-making process can often have conflicting characteristics. For example, while a strategy may be highly effective from a technical standpoint, it might also be unsustainable from a cost perspective. Alternatively, a user-friendly system may have a low security level. In such conflicting situations, decision-makers need to identify the most balanced option according to their subjective priorities and objectives. At this point, MCDM methods enable decision-makers to conduct a more holistic and consistent evaluation by offering them the opportunity to weight various criteria and compare alternatives based on those criteria [42].

MCDM methods are approaches that assist individuals in making decisions under uncertainty [9]. In today's rapidly changing and unpredictable conditions, decision-makers are often forced to make choices without possessing complete information. Uncertainty can stem from both environmental conditions and a lack of foresight regarding the future performance of alternatives. In such cases, since intuition-based decisions can lead to erroneous outcomes, MCDM methods can be extremely useful for reducing uncertainty and making decisions based on more solid foundations. These methods transform a decision-maker's knowledge into a systematic structure, taking into account both subjective and objective data, thereby providing a holistic approach to the decision-making process [43-44]. In this study, Pythagorean Fuzzy AHP (PFAHP) and Neutrosophic Fuzzy AHP (NFAHP) were utilized.

3.1. Pythagorean Fuzzy AHP

In solving MCDM problems involving uncertainty today, the development of methods that can more effectively reflect the intuitive judgments of decision-makers has gained importance. In this context, the AHP, designed by Prof. Thomas L. Saaty, has been one of the fundamental methods used for modeling decision structures and prioritizing alternatives [45]. However, the classical AHP method can be inadequate, especially in situations where subjective assessments are prominent, as it forces decision-makers to express their judgments with precise numbers.

To overcome this limitation, the Fuzzy AHP method was developed, emerging from the integration of AHP with fuzzy logic. In this method, decision-makers can make comparisons using linguistic variables instead of numerical values, and these expressions are modeled with fuzzy numbers. Thus, the decision-making process achieves a more flexible and realistic structure. Pythagorean fuzzy numbers are particularly preferred in evaluation processes where subjective judgments are prominent. This structure, which allows decision-makers to make their comparisons between alternatives or criteria with more flexible linguistic terms, provides high precision in decisions where quantitative and qualitative data are processed together. When the hierarchical decision model of AHP is combined with Pythagorean fuzzy logic, the decision-making process becomes both systematic and resilient to uncertainty. The linguistic variables to be used are given in Table 1.

Table 1. Linguistic Variables for Pythagorean Fuzzy AHP [43]

Linguistic Variables		Interval-valued Pythagorean Fuzzy Numbers			
		Lowest Membership (uL)	Highest Membership (uU)	Lowest Non-Membership (vL)	Highest Non-Membership (vU)
Absolutely Low	**AL**	0,0	0,0	0,9	1,0
Very Low	**VL**	0,1	0,2	0,8	0,9
Low	**L**	0,2	0,35	0,65	0,8
Below Average	**BA**	0,35	0,45	0,55	0,65
Equal	**E**	0,1965	0,1965	0,1965	0,1965
Average	**A**	0,45	0,55	0,45	0,55
Above Average	**AA**	0,55	0,65	0,35	0,45
High	**H**	0,65	0,8	0,2	0,35
Very High	**VH**	0,8	0,9	0,1	0,2
Absolutely High	**AH**	0,9	1,00	0,00	0,00

PFAHP was chosen for this study particularly because it offers the ability to establish a more flexible relationship between membership and non-membership degrees. This approach enabled both a more accurate modeling of expert opinions and a reliable weighting of the decision criteria. The steps of the PFAHP are presented in Figure 1.

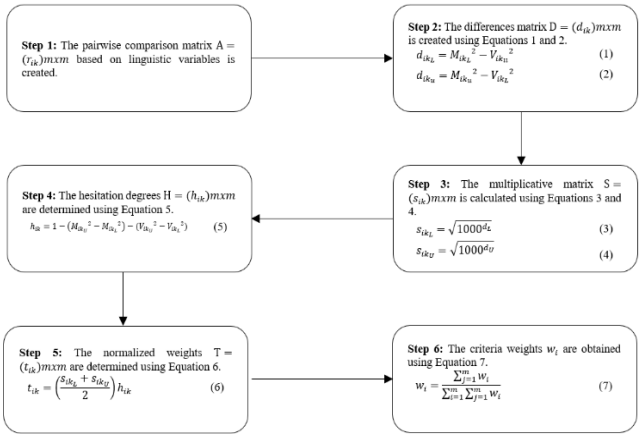

Figure 1. Steps of Pythagorean Fuzzy AHP [43]

3.2. Neutrosophic Fuzzy AHP

In complex decision-making problems, classical decision support systems can be inadequate, especially in situations characterized by a lack of information, uncertainty, and conflicting judgments. For this reason, there has been a need to develop methods that more accurately reflect the uncertainty-laden expressions of decision-makers within the model. Accordingly, the Neutrosophic logic approach was developed and has been integrated into decision-making techniques. Neutrosophic logic has the ability to incorporate elements of fuzziness and indeterminacy, as well as inconsistencies, into the mathematical model [44].

Although the AHP is a structured method frequently used in the MCDM field, it expects the decision-maker to express all evaluations with precise ratios [46]. This situation creates limitations, particularly in areas where subjective and intuitive judgments are dominant. Therefore, integrating AHP with different logic systems allows for the creation of more flexible and comprehensive decision models [45].

The NFAHP method, developed in this context, combines both the hierarchical structure of classical AHP and the multi-dimensional uncertainty modeling capability of Neutrosophic logic. In this way, characteristics such as indeterminacy and inconsistency, which are difficult to represent in classical models, can be directly modeled with Neutrosophic structures. In the NFAHP method, decision-makers are required to make inter-criteria comparisons using linguistic terms. These terms are represented by interval Neutrosophic numbers, and an evaluation matrix is constructed. Subsequently, the weights are calculated to determine the relative importance of the criteria. This process directly incorporates the decision-maker's conflicting views into the evaluation process, rather than suppressing them. The linguistic variables to be used are given in Table 2.

Table 2. Linguistic Variables for Neutrosophic AHP [44]

Linguistic Term		Neutrosophic Set					
Equal Importance	**EI**	0,50	0,50	0,50	0,50	0,50	0,50
Weakly More Important	**WMI**	0,50	0,60	0,35	0,45	0,40	0,50
Moderate Importance	**MI**	0,55	0,65	0,30	0,40	0,35	0,45
Moderately More Important	**MMI**	0,60	0,70	0,25	0,35	0,30	0,40
Strong Importance	**SI**	0,65	0,75	0,20	0,30	0,25	0,35
Strongly More Important	**SMI**	0,70	0,80	0,15	0,25	0,20	0,30
Very Strong Importance	**VSI**	0,75	0,85	0,10	0,20	0,15	0,25
Very Strongly More Important	**VSMI**	0,80	0,90	0,05	0,10	0,10	0,20
Extreme Importance	**XI**	0,90	0,95	0,00	0,05	0,05	0,15
Extremely High Importance	**EHI**	0,95	1,00	0,00	0,00	0,00	0,10
Absolutely More Important	**AMI**	1,00	1,00	0,00	0,00	0,00	0,00

The NFAHP method is particularly effective in complex systems where the simultaneous evaluation of conflicting information sources is necessary. This method allows for a more realistic evaluation process by defining the decision-makers' degrees of truth (confidence), indeterminacy, and falsity (potential erroneous judgments).

The steps of the NFAHP are presented in Figure 2.

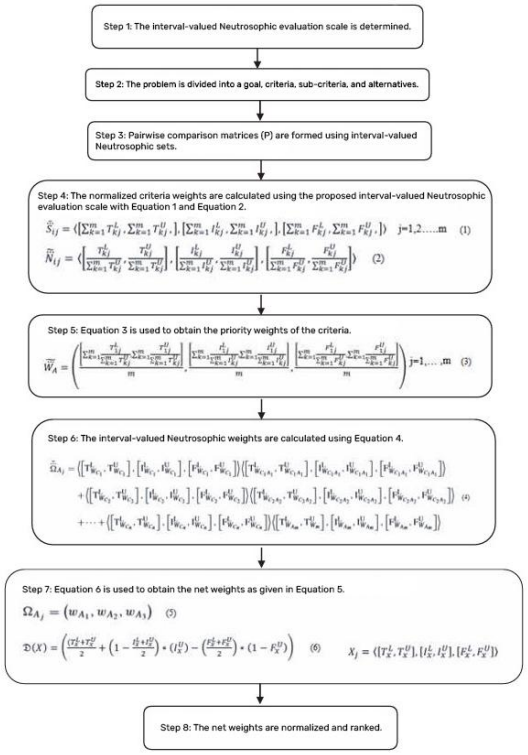

Figure 2. Steps of Neutrosophic Fuzzy AHP [44]

3.3. TOPSIS Method

TOPSIS is a widely used method in MCDM problems that offers decision-makers a systematic evaluation framework. The method aims to identify the alternative that is closest to the ideal solution and farthest from the negative-ideal solution. Through this approach, the distance of each alternative from the positive-ideal and negative-ideal solutions is calculated to obtain relative proximity values. The alternatives are ranked based on these values, and the most suitable option is determined. TOPSIS provides robust decision support, particularly in problems where there is a large number of decision criteria and conflicting situations exist. Due to its ability to determine the most suitable alternative for each criterion using simple calculations and to produce a highly reliable ranking, the TOPSIS method is frequently one of the most preferred methods [47]. The steps of the TOPSIS method are as shown in Figure 3.

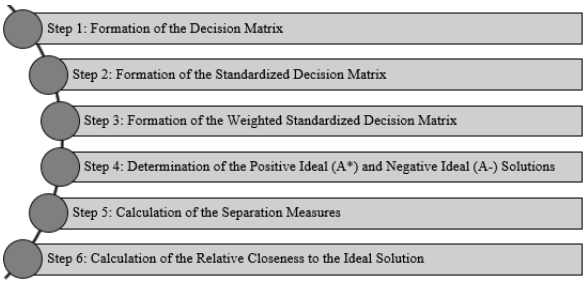

Figure 3. Steps of the TOPSIS Method [10]

3.4. PROMETHEE Method

PROMETHEE is a MCDM method developed by Jean-Pierre Brans in 1982. In MCDM problems where alternatives need to be evaluated through pairwise comparisons, the PROMETHEE method offers a highly effective and systematic approach. In this method, the preference degree of each alternative is determined by comparing it with the others, and from these comparisons, positive and negative flow values are calculated. With the help of these obtained values, the alternatives can be clearly ranked. As the method allows the decision-maker to define preference functions, it permits the joint evaluation of both subjective and objective judgments. Thus, it provides a strong analytical framework, especially in problems involving conflicting criteria. PROMETHEE is a system designed for selecting the most suitable alternative according to the criteria [48]. The steps of the PROMETHEE method are as shown in Figure 4.

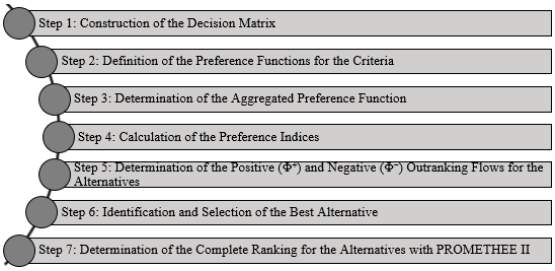

Figure 4. Steps of the PROMETHEE Method [48]

4. LITERATURE REVIEW

Some studies conducted on cybersecurity and phishing attacks are as follows:

In their study, A Bose et al. (2008) evaluated the preparedness levels of banks in Hong Kong against phishing attacks. In the study, the websites of banks registered in Hong Kong were analyzed and scored based on the criteria of accessibility, usability, and information content [49].

In his study, Hekim (2015) examines phishing attacks from technical, historical, and legal perspectives, analyzing how individuals' personal and financial information is obtained through social engineering techniques. The study draws particular attention to targeted spear phishing and whaling attacks, and alongside technical protection methods like user education, SSL certificates, and URL verification, it criticizes the inadequacies of legal regulations in Turkey. In conclusion, it is emphasized that a multi-layered approach (user awareness, technical measures, legal reforms, and international cooperation) should be adopted in the fight against phishing [50].

In their study, Yalçın and Avşar (2018) explain common attack types such as phishing, whaling (phishing targeting senior executives), vishing (voice phishing), and reverse social engineering, presenting example scenarios for each. The study noted the importance of human-focused security training and awareness activities, equally as much as technical measures, in countering social engineering attacks [51].

In their study, Efe et al. (2019) determined that there has been an increase in SWIFT and phishing attacks within mobile banking systems. The study provides recommended fundamental security strategies against these attacks. Some of these strategies include email and web page personalization, two-step authentication, advanced security software (antivirus and anti-spyware systems), a multi-layered security architecture, regular software/hardware updates, strong password policies, multi-factor authentication systems, annual penetration tests, cyber incident response plans, and personnel training programs. They mentioned that recommended behavioral measures for users include avoiding suspicious links, protecting personal information, and adhering strictly to security protocols [37].

In his study, Alanezi (2021) emphasizes the critical role of the internet in social and financial life and examines the phishing threats faced by organizations, particularly those that conduct online transactions. The research analyzes current phishing detection methods against risks such as financial losses, data breaches, and reputational damage, and focuses on the shortcomings in the anti-phishing field by comparatively evaluating studies from the last four years [52].

In his study, Arslan (2021) conducted a two-phase drill on 33,000 employees at a public institution to measure user awareness against phishing attacks. In the study, user behavior was analyzed using fake emails, malicious file download scenarios, and USB drives. The results showed that 17.3% of field personnel and 29.6% of managers were vulnerable to phishing attacks. Although it was noted that machine learning-based phishing prevention systems are promising, the human factor was observed to remain the weak link [53].

In his doctoral thesis, Eren (2023) conducted a comprehensive study to fill a gap in the literature by examining the determining factors of cybersecurity awareness in the banking sector and its effects on employees. Existing cybersecurity studies in payment

systems and banking were analyzed, the situation in the Turkish banking sector was evaluated as a case study, and an awareness model was proposed to increase employees' cybersecurity consciousness. Furthermore, policy recommendations were developed to improve the results of mandatory practices like social engineering tests, and contributions were made to academia and industry stakeholders by presenting components that would enable end-users (bank employees and customers) to use technology consciously [54].

In their study, Kör and Erdoğa (2023) examine the historical development of phishing attacks and the current threat landscape. The study first explains in detail the fundamental mechanisms of phishing attacks and the methods used (SMS, email, social media messages). The research systematically presents the practical measures that individuals and institutions can take against phishing attacks [55].

In their study, Çon and Arıca (2024) examined the development of digital banking in Turkey and global trends. While cost-effectiveness, accessibility, and fast service are among the greatest advantages of digital banking, security risks were highlighted as a significant weakness. They stated that threats such as cyber-attacks, phishing attempts, and data theft are among the primary security risks facing digital banking [39].

In their study, Doing et al. (2024) examined the reporting behaviors of employees at a bank concerning phishing emails. In 50,000 reports collected over 16 months, it was observed that employees frequently reported benign emails (35%) as well as malicious ones (26%). Training and simulations temporarily increased the reporting of benign emails but did not affect the recognition rate of real threats. The study emphasized the importance of prompt reporting of suspicious emails and feedback mechanisms, recommending more effective strategies for organizations in the fight against phishing [56].

In his master's thesis, Erdoğan (2024) examines academic studies conducted in the field of cybercrime between 2000 and 2023 using the bibliometric analysis method. Motivated by the growing importance of cybercrime and the need for a systematic evaluation of research in this field, the study analyzed 2,566 academic publications obtained from the Web of Science database [57].

In their study, Nguyen et al. (2024) used MCDM methods to assess cybersecurity risks in Vietnam's finance and banking sector and to determine the most effective preventive strategies. The study aimed to increase decision accuracy and reliability by combining the DELPHI, DEMATEL, and COCOSO methods with Neutrosophic Sets and Z-number concepts [58].

In their study, Yasmin et al. (2024) examined the increasing risks of phishing in banking services undergoing digital transformation in Indonesia, with a particular focus on state-owned banks (Bank BUMNs). The research analyzes how phishing attacks occur and the risks faced by banks and customers, highlighting system security vulnerabilities and low awareness levels. The study recommends measures such as two-factor authentication, regular security audits, customer education, and cross-sector collaboration. It also concludes that there is a need to increase the public's level of awareness regarding phishing [59].

In his study, Yıldırım (2024) examined in detail the risks encountered in digital banking and remote identity verification processes and presented solution proposals. He addressed critical issues such as phishing attacks, the misuse of Deep Fake technology, biometric data security, operational vulnerabilities, and shortcomings in legal regulations. The study recommended strong authentication methods to enhance the security of remote identity verification, such as AI-supported fraud detection, multi-factor authentication (MFA), biometric systems integrated with NFC technology, and SIM OTP [60].

In their study, Yuspin et al. (2024) analyzed the increasing phishing attacks in Indonesia's digital banking sector and the impacts of these attacks on customer security and legal systems. They explained that existing legal regulations are inadequate and why phishing incidents are on the rise. The study emphasizes that digital banks can mitigate risks through measures such as customer education, two-factor authentication, and real-time cybersecurity systems [61].

In their study, Adejumo and Ogburie (2025) addressed the advantages brought by the digitalization of financial services as well as the emerging cybersecurity risks (phishing attacks, data breaches, ransomware, etc.) and examined solutions like AI-based fraud detection, blockchain, and multi-factor authentication to ensure financial transaction security [2].

In their study, Cele et al. (2025) conducted a systematic literature review to identify cybersecurity threats that hinder the adoption of digital banking and to present sustainable strategies for combating these risks in the banking sector. Within the scope of the research, 58 articles published between 2015 and 2023 were reviewed, and the negative impacts of phishing, vishing, identity theft, and malware attacks on the adoption of digital banking were emphasized. The study recommended 13 fundamental strategies, such as increasing customer awareness, implementing strong password policies, using secure software, and organizing training programs [62].

In an article by Çözümpark (URL1), what phishing attacks are, how to recognize them, and how they can be prevented are explained. While emphasizing that cybercriminals attempt to steal personal information through fake emails, messages, and websites, the article recommends precautions to protect against such attacks, such as not opening suspicious links and using two-step verification [63].

In their article, Gais Security (URL2) explains in detail the fundamental mechanisms, types, and protection methods of phishing attacks. The article particularly focuses on email-based phishing, smishing, vishing, and targeted spear phishing techniques. The article offers practical tips on how to identify these attacks while emphasizing fundamental protection strategies like two-factor authentication, checking suspicious links, and user education. Additionally, the steps to be followed when exposed to a phishing attack are also summarized [64].

In its article, Güney Bilişim (URL3) addresses the dangers of phishing and social engineering attacks in the digital world. The article explains with examples the methods used by cybercriminals to steal personal information or infiltrate systems (such as fake emails, creating a sense of urgency, and impersonating trusted institutions), and emphasizes the material and non-material impacts of these attacks on individuals and organizations. Furthermore, it highlights the importance of awareness against cyber threats by listing basic security measures that users can take (such as not opening suspicious links, using two-factor authentication, and updating passwords regularly) [65].

In this context, the study provides decision support for financial institutions in selecting appropriate cybersecurity strategies against phishing attacks, while also contributing to the literature by proposing an integrated and comparative decision-making framework. Specifically, PFAHP and NFAHP methods are employed to determine the weights of the evaluation criteria, and TOPSIS and PROMETHEE methods are applied to rank the alternatives based on these weights. Through this approach, it is aimed to achieve a more reliable and comprehensive evaluation of cybersecurity strategies under uncertainty and to offer a practical framework for strategy selection in the financial sector.

5. APPLICATION

The solution to the problem followed the systematic framework specified in Figure 5. After the problem was defined, data were collected for the application of the MCDM methods.

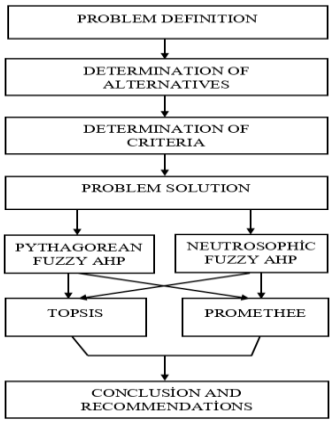

Figure 5. Application Flowchart

5.1. Problem Definition

The financial sector has become an attractive target for cyber attackers due to its high transaction volume and valuable customer data. In this context, phishing attacks, in particular, pose serious threats such as accessing sensitive information by deceiving employees, infiltrating systems with malicious software, and initiating fraudulent activities. In banking systems, the joint evaluation of technical and structural security measures, in addition to user awareness, is of critical importance for developing an effective defense against these attacks. Therefore, the selection of the most suitable anti-phishing strategy by financial institutions, using their existing resources in the most efficient manner, emerges as a decision problem.

Within the scope of the study, expert evaluations were obtained through face-to-face group interview sessions. In these sessions, experts shared their knowledge and experience regarding cybersecurity strategies, and their judgments were incorporated into the decision-making process. The use of a face-to-face group interview technique enabled a more interactive and in-depth evaluation environment, allowing experts to discuss different perspectives and reach more consistent assessments. Information regarding the expert group that was formed is provided in Table 3. The table shows the experts' professional fields and the number of years of experience in the sector.

Table 3. Expert List

Expert No	Expert Category	Experience (Years)
E1	**Academician**	20
E2	**Graduate Student (Industrial Engineer)**	3
E3	**Information Security Manager**	11
E4	**Cyber Security Expert 1**	8
E5	**Cyber Security Expert 2**	7

5.2. Determination of Alternatives

Seven different strategies aimed at preventing phishing attacks have been identified. These strategies are as follows [57-64-65]:

- **Employee Training (ET):** These are training sessions organized to ensure employees are aware of phishing attacks and act accordingly. In these trainings, employees are taught how to distinguish suspicious emails, the importance of not clicking on malicious links, and how to protect personal information. Thus, employees become more vigilant against attacks, and erroneous behaviors are prevented.
- **E-mail Filtering (EMF):** These are AI-supported systems that enable the detection and blocking of phishing emails before they reach the user. The established filters separate spam and malicious

messages and block their attachments. As a result, risky emails do not land directly in users' inboxes.

- **Multi-Factor Authentication (MFA):** This is a security method where, instead of using only a password to log in, users are required to complete second or third verification steps. This makes it more difficult for attackers to access the system.
- **Segregation of Duties (SD):** This is the practice of not granting a single staff member access to all systems or critical data. Privileges are separated according to duties and responsibilities. This way, even if a user's account is compromised, the attacker can only operate within the areas accessible to that individual and cannot control the entire system.
- **Endpoint Security (ES):** This involves securing user devices such as computers or phones. These systems monitor the software running and operations performed on the devices, detect suspicious activities, and prevent the spread of malicious software.
- **Zero Trust (ZT):** This is the principle of not automatically trusting any user or device, whether internal or external to the organization. Every access request is verified and controlled. This method largely prevents even compromised accounts from moving freely within the system.
- **DNS Filtering and Web Security (DNSFWS):** Even if personnel accidentally click on a malicious link, this system blocks access to harmful websites. DNS filtering blocks the addresses of malicious sites and protects the user from harmful content.

5.3. Determination of Criteria

Six criteria have been established to evaluate the strategies. These criteria are as follows [1-3-58]:

- **Effectiveness (E):** This refers to how successfully the strategy prevents phishing attacks. Questions such as whether the implemented defense method can stop phishing attempts and whether it can reduce the damage from an attack are evaluated within this scope. An effective strategy prevents an attack from reaching the system or being successful.
- **Cost (C):** This refers to the total cost required to implement and sustain the strategy. If protection is to be provided through a software package, elements such as license fees, infrastructure investments, training expenses, and personnel support are considered within this scope. Since institutions must prioritize solutions that fit their budgets, cost is a significant determining factor.
- **Implementation Difficulty (ID):** This refers to the challenges in implementing the planned strategy. These challenges include issues such as technical skill/manpower, resources, time, and the level of complexity.
- **Sustainability (SU):** This refers to whether a strategy can remain effective and up to date not just initially, but also in the long term. In today's world, where technology and attack methods are constantly changing, sustainable strategies must be able to endure both technically and organizationally.
- **User Acceptance (UA):** This indicates the extent to which the strategy will be adopted by the institution's employees. Solutions that are cumbersome or disrupt workflows are not well-received by users. This, in turn, reduces the efficiency of the system. Therefore, user compliance with the strategies is an important evaluation criterion.
- **Scope (SC):** This indicates whether the strategy is effective only against specific types of phishing attacks or against all varieties of attacks. A method effective only against email-based threats may be inadequate against other types of phishing attacks, such as those based on phone calls or social media. This criterion shows how broad an impact area the solution has.

5.4. Problem Solution

Because this problem involves numerous alternatives and criteria, a systematic approach was taken by applying fuzzy MCDM methods, namely PFAHP, NFAHP, TOPSIS, and PROMETHEE. The initial matrix and the subsequent weights are provided below.

5.4.1. Pythagorean Fuzzy AHP

The initial matrix for the PFAHP method is as given in Table 4. After determining the initial matrix, the steps to be applied are given in Figure 1.

Table 4. Pythagorean Fuzzy AHP Initial Matrix

Pairwise Comparison with Linguistic Variables	**Criteria**					
	E	**C**	**ID**	**S**	**UA**	**SC**
E	E	H	VH	AA	AA	AA
C	L	E	AA	BA	BA	BA
ID	VL	OA	E	BA	BA	L
SU	BA	AA	AA	E	AA	A
UA	BA	AA	AA	BA	E	BA
SC	BA	AA	H	A	AA	E

As a result, the normalized weight of each criterion has been calculated as specified in Table 5.

Table 5. Pythagorean Fuzzy AHP Weights

Criteria	**Weights**
Effectiveness (E)	0,283956055
Cost (C)	0,101804408
Implementation Difficulty (ID)	0,062008097
Sustainability (SU)	0,180927615
User Acceptance (UA)	0,139320127
Scope (SC)	0,231983698

The weights reflect the relative importance of the criteria in the decision-making process. In this study, the criterion with the highest weight was identified as Effectiveness, with 28.4%, indicating that it is the primary criterion. This result can be attributed to the fact that phishing attacks in the financial sector can lead to severe consequences such as financial losses, data breaches, and reputational damage. Therefore, strategies are primarily evaluated based on their ability to prevent such threats. In this context, it can be inferred that decision-makers prioritize the capability of strategies to mitigate and prevent attacks over secondary factors such as cost and implementation difficulty.

The criteria weights were found to be in the following order: Effectiveness > Scope > Sustainability > User Acceptance > Cost > Implementation Difficulty.

5.4.2 Neutrosophic Fuzzy AHP

The initial matrix for the NFAHP method is as given in Table 6. After determining the initial matrix, the steps to be applied are given in Table 6.

Table 6. Neutrosophic Fuzzy AHP Initial Matrix

Pairwise Comparison with Linguistic Variables	**E**	**C**	**ID**	**SU**	**UA**	**SC**
E	EI	SMI	XI	WMI	MI	WMI
C	-	EI	WMI	-	-	-
ID	-	-	EI	-	-	-
SU	-	WMI	MI	EI	WMI	EI
UA	-	WMI	WMI	-	EI	-
SC	-	MI	SMI	-	WMI	EI

In the final step, the calculated net weights were normalized to make them comparable and are ranked in order of importance in Table 7.

Table 7. Neutrosophic Fuzzy AHP Weights

Criteria	**Weights**	**Rank**
Effectiveness (E)	0,18042	1
Cost (C)	0,15935	5
Implementation Difficulty (ID)	0,15011	6
Sustainability (SU)	0,16975	3
User Acceptance (UA)	0,16656	4
Scope (SC)	0,17382	2

As a result of the calculations, the criteria weight ranking from the NFAHP method was as follows: Effectiveness > Scope > Sustainability > User Acceptance > Cost > Implementation Difficulty. The Effectiveness criterion, with 18.04%, was determined to be the most important criterion.

The same ranking emerged from both criteria weighting methods. When the two tables are compared, striking differences are observed between the weights obtained for the same criteria using different methods. Specifically, while the Effectiveness criterion had a weight far superior to the others according to the PFAHP method, it had a more balanced distribution in the NFAHP method. The Implementation Difficulty criterion, which was insignificant in the PFAHP method, became one of the determining criteria in the NFAHP method. The significant variation in the weights of the Cost and Scope criteria depending on the method demonstrates how different analytical approaches can affect decision-making processes and criteria prioritization in various ways.

The criteria weights determined by PFAHP and NFAHP will be used in the solution phase of the TOPSIS and PROMETHEE methods.

5.4.3 TOPSIS Method

To ensure the correct application of the TOPSIS method, the data for the evaluated strategies were normalized using a scoring method. The decision matrix is given in Table 8.

Table 8. TOPSIS Decision Matrix

Decision Matrix	**E**	**C**	**ID**	**SU**	**UA**	**SC**
ET	92	100	100	68	82	88
EMF	97	90	92	100	100	76
MFA	100	73	93	90	85	85
SD	88	75	76	85	84	90
ES	85	65	78	86	85	79
ZT	92	62	67	93	68	100
DNSFWS	76	86	89	80	89	79

Using the given decision matrix, the result was determined by applying the weights found from the PFAHP and NFAHP methods. The solution obtained using the PFAHP method weights, ranked in descending order, is given in Table 9.

Table 9. PFAHP-TOPSIS Results Matrix

Criteria	**Weights**
E-mail Filtering (EMF)	0,597484
Multi-Factor Authentication (MFA)	0,570218
Zero Trust (ZT)	0,5224
Employee Training (ET)	0,490143
Segregation of Duties (SD)	0,468126
DNS Filtering and Web Security (DNSWSF)	0,386944
Endpoint Security (ES)	0,316196

The TOPSIS solution, obtained using the NFAHP method weights and ranked in descending order, is given in Table 10.

Table 10. NFAHP-TOPSIS Results Matrix

Criteria	Weights
E-mail Filtering (EMF)	0,685121
Employee Training (ET)	0,609162
Multi-Factor Authentication (MFA)	0,552172
DNS Filtering and Web Security (DNSFWS)	0,529906
Segregation of Duties (SD)	0,451537
Zero Trust (ZT)	0,365854
Endpoint Security (ES)	0,329996

It was observed that the E-mail Filtering alternative ranked highest in this method's weight. Conversely, Endpoint Security was observed to be the worst alternative in both cases. The Employee Training strategy ranked 4th according to the PFAHP-TOPSIS result, but 2nd according to the NFAHP-TOPSIS result. The reason for this was determined to be that the weights of the Cost and Implementation Difficulty criteria were low in the PFAHP method, whereas they were high in the NFAHP method. This indicates that strategies such as Employee Training, which are relatively easier to implement and more cost-efficient, tend to achieve higher rankings when these criteria are assigned greater importance.

5.4.4. PROMETHEE Method

The PROMETHEE method was solved using the Visual PROMETHEE (Version 1.4.0.0) software package. Two solutions were implemented using the weights from both methods (PFAHP and NFAHP). The data interface of the Visual PROMETHEE software is given in Figure 6.

Scenario1	Effectiveness	Cost	Implementati...	Sustainability	User Accept...	Scope
Unit	unit	unit	unit	unit	unit	unit
Cluster/Group	◆	◆	◆	◆	◆	◆
Preferences						
Min/Max	max	max	max	max	max	max
Weight	0,28	0,10	0,06	0,18	0,14	0,23
Preference Fn.	Linear	Linear	Linear	Linear	Linear	Linear
Thresholds	absolute	absolute	absolute	absolute	absolute	absolute
- Q: Indifference	1,00	1,00	1,00	1,00	1,00	1,00
- P: Preference	2,00	2,00	2,00	2,00	2,00	2,00
- S: Gaussian	n/a	n/a	n/a	n/a	n/a	n/a
Statistics						
Minimum	76,00	62,00	67,00	68,00	68,00	76,00
Maximum	100,00	100,00	100,00	100,00	100,00	100,00
Average	90,00	78,71	84,57	86,00	84,71	85,29
Standard Dev.	7,39	12,80	10,63	9,43	8,78	7,67
Evaluations						
Employee Training	92,00	100,00	100,00	68,00	82,00	88,00
Email Filtering Sy...	97,00	90,00	92,00	100,00	100,00	76,00
Multi-Factor Aut...	100,00	73,00	93,00	90,00	85,00	85,00
Segregation of D...	88,00	75,00	76,00	85,00	84,00	90,00
Endpoint Security	85,00	65,00	78,00	86,00	85,00	79,00
Zero Trust Appro...	92,00	62,00	67,00	93,00	68,00	100,00
DNS Filtering and...	76,00	86,00	86,00	80,00	89,00	79,00

Figure 6. Visual PROMETHEE Interface

The results, according to the PFAHP method criteria weights, are given in Figure 7.

PROMETHEE Flow Table

Rank	action	Phi	Phi+	Phi-
1	Email Filtering Systems	0,3765	0,6831	0,3066
2	Multi-Factor	0,3413	0,6423	0,3009
3	Zero Trust Approach	0,0967	0,5247	0,4280
4	Employee Training	0,0147	0,4837	0,4690
5	Segregation of Duties	-0,0115	0,4559	0,4675
6	DNS Filtering and Web	-0,3937	0,2838	0,6775
7	Endpoint Security	-0,4240	0,2304	0,6544

Figure 7. PFAHP-PROMETHEE Method Results

According to the results, the most important strategy was determined to be E-mail Filtering, and the strategy with the worst rank of importance was Endpoint Security.

The results according to the NFAHP method criteria weights are given in Figure 8.

PROMETHEE Flow Table

Rank	action	Phi	Phi+	Phi-
1	Email Filtering Systems	0,4640	0,7195	0,2555
2	Multi-Factor	0,2590	0,5892	0,3302
3	Employee Training	0,1167	0,5433	0,4266
4	Segregation of Duties	-0,0726	0,4218	0,4944
5	Zero Trust Approach	-0,1589	0,4055	0,5644
6	DNS Filtering and Web	-0,2164	0,3773	0,5937
7	Endpoint Security	-0,3918	0,2477	0,6395

Figure 8. NFAHP-PROMETHEE Method Results

According to the results of the PFAHP-PROMETHEE method, E-mail Filtering was identified as the most prioritized strategy. This was followed by Multi-Factor Authentication (MFA) and the Zero Trust approach, respectively. The lowest-performing alternative was determined to be Endpoint Security. Figure 9 was obtained by comparing the results with those obtained using the PFAHP-TOPSIS method.

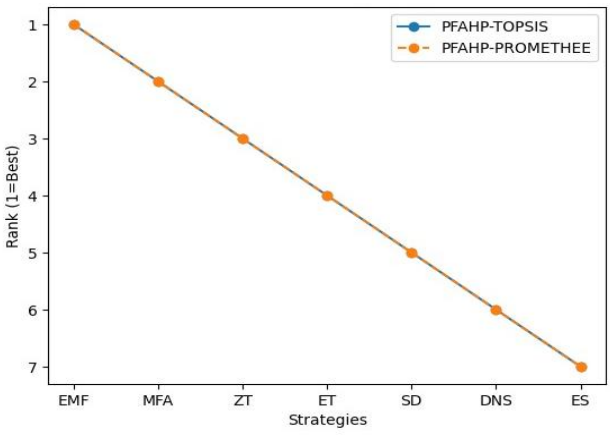

Figure 9. PFAHP-Based Ranking Comparison

When the results based on the PFAHP method are evaluated, a higher level of consistency is observed between the TOPSIS and PROMETHEE results. In both approaches, E-mail Filtering is ranked as the best alternative, while Endpoint Security is consistently the worst. In addition, the top three strategies—E-mail Filtering, Multi-Factor Authentication (MFA), and Zero Trust—maintain the same ranking order in both methods. This strong alignment suggests that the results obtained under the Pythagorean fuzzy framework are highly consistent and that the identified leading strategies are robust across different evaluation methods.

Similarly, a comparison of the NFAHP-PROMETHEE results with those obtained using NFAHP-TOPSIS is shown in Figure 10.

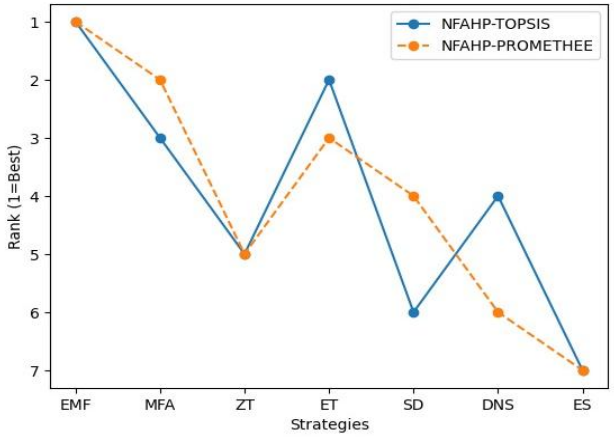

Figure 10. NFAHP-Based Ranking Comparison

When the results obtained from the NFAHP-based approaches are examined, it is observed that E-mail Filtering ranks first in both the TOPSIS and PROMETHEE methods. Similarly, Endpoint Security is identified as the lowest-ranked alternative in both methods. Although minor differences exist in the intermediate rankings, the consistency in the best and worst alternatives indicates that the results obtained under the Neutrosophic framework are stable and reliable across different ranking techniques.

6. CONCLUSION AND RECOMMENDATIONS

In this study, an analytical solution approach was presented for evaluating applicable cybersecurity strategies against frequently encountered phishing attacks in the financial sector, utilizing the MCDM methods of PFAHP, NFAHP, TOPSIS, and PROMETHEE. Six decision criteria—namely effectiveness, cost, implementation difficulty, sustainability, user acceptance, and scope—were weighted using the PFAHP and NFAHP methods. Strategy selection from among 7 alternatives was performed using the TOPSIS and PROMETHEE methods.

Based on the findings from both fuzzy AHP methods, the "effectiveness" criterion, in particular, was identified as the criterion with the highest importance in both methods. This situation indicates that effectiveness is a priority in the selection of security strategies in the sector. On the other hand, the lower importance of operational factors such as "cost" and "implementation difficulty" suggests that institutions prioritize an effective defense over economic concerns in their security strategies. In the TOPSIS and PROMETHEE methods, the prominent strategy was identified as E-mail filtering, while the worst strategy was Endpoint Security.

Based on the findings of this study, it is recommended that financial institutions primarily turn to strategies that are highly effective and more comprehensive against phishing attacks. As a priority strategy, E-mail Filtering is recommended. Subsequently, importance should be given to the MFA strategy.

As recommendations for future studies, the application levels of strategies in different sectors can be examined, criteria weights can be diversified with expert opinions, and analyses can be deepened with integrated MCDM approaches. Furthermore, it will be possible to make more accurate and pertinent evaluations by creating strategy sets specific to different threat types.

ACKNOWLEDGMENT

The authors would like to thank Eren Batu GÜNAYDIN, an M.Sc. student in the Department of Industrial Engineering at Kirikkale University, for his valuable contributions to this study.

REFERENCES

[1] T. Kandemir, H. Karataş, "Ticari bankaların finansal performanslarının çok kriterli karar verme yöntemleri ile incelenmesi: Borsa İstanbul'da işlem gören bankalar üzerine bir uygulama (2004-2014)", *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 5(7), 1766-1776, 2016.

[2] A. Adejumo, C. Ogburie, "Strengthening finance with cybersecurity: Ensuring safer digital transactions", *World Journal of Advanced Research and Reviews*, 25, 2025.

[3] M. M. Ali, N. F. Mohd Zaharon, "Phishing—A cyber fraud: The types, implications and governance", *International Journal of Educational Reform*, 33(1), 101-121, 2024.

[4] S. Hasham, S. Joshi, D. Mikkelsen, **Financial crime and fraud in the age of cybersecurity**, McKinsey & Company, 2019.

[5] M. A. Ivanov, B. V. Kliuchnikova, I. V. Chugunkov, A. M. Plaksina, "Phishing attacks and protection against them", 2021 **IEEE conference of russian young researchers in electrical and electronic engineering (ElConRus)**, 425-428, Ocak 2021.

[6] A. L. Johnson, "Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation", NC Banking Inst., 20, 277, 2016.

[7] T. Savaş, S. Savaş, "Tekdüzen kaynak bulucu yoluyla kimlik avı tespiti için makine öğrenmesi algoritmalarının özellik tabanlı performans karşılaştırması", Politeknik Dergisi, 1-1, 2021.

[8] A. K. Jain, B. B. Gupta, "Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation", *International Journal of Information and Computer Security*, 10(4), 398-417, 2018.

[9] H. Dinçer, S. Yüksel, "Çok Kriterli Karar Verme Yöntemlerinin finans sektöründeki uygulamasına yönelik yapılmış çalışmaların analizi", *Ekonomi İşletme ve Maliye Araştırmaları Dergisi*, 1(1), 1-16, 2018.

[10] B. Saçan, T. Eren, "Dijital pazarlama strateji seçimi: SWOT analizi ve çok ölçütlü karar verme yöntemleri", *Politeknik Dergisi*, 25(4), 1411-1421, 2021.

[11] M. Karahan, L. Kızkapan, "Çok Kriterli Karar Verme Teknikleriyle Bankaların Finansal Performanslarının Karşılaştırmalı Analizi", *Verimlilik Dergisi*, (3), 441-462, 2022.

[12] M. Taş, Ş. N. Özlemiş, M. Hamurcu, T. Eren, "Ankara'da AHP ve PROMETHEE yaklaşımıyla monoray hat tipinin belirlenmesi", *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 3(1), 65-89, 2017.

[13] K. N. Johnson, "Cyber risks: Emerging risk management concerns for financial institutions", Ga. L. Rev., 50, 131, 2015.

[14] M. S. Öztürk, "Siber Saldirilar, Siber Güvenlik Denetimleri ve Bütüncül bir Denetim Modeli Önerisi", *Journal of Accounting and Taxation Studies*, 208-232, 2018.

[15] Ö. Akçakanat, O. Özdemir, M. Mazak, "İşletmelerde siber güvenlik riskleri ve bilgi teknolojileri denetimi: bankaların siber güvenlik uygulamalarının incelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5(2), 246-270, 2021.

[16] N. Abid, "Ransom Ware Attacks on Financial Institutions: A Review of the Literature on Cybersecurity Risks and Countermeasures", *International Journal of Multidisciplinary Sciences and Arts*, 2(2), 164-169, 2023.

[17] E. Ekşioğlu, "Teknoloji ve işbirliği arasındaki ilişki", *Studies On Social Science İnsights*, 1, 35-50, 2025.

[18] S. Mohurle, M. Patil, "A brief study of wannacry threat: Ransomware attack 2017", *International journal of advanced research in computer science*, 8(5), 1938-1940, 2017.

[19] A. Abhishta, W. van Heeswijk, M. Junger, L. J. Nieuwenhuis, R. Joosten, "Why would we get attacked? An analysis of attacker's aims behind DDoS attacks", *Journal of wireless mobile networks, ubiquitous computing, and dependable applications*, 11(2), 3-22, 2020.

[20] G. Mazzarolo, A. D. **Jurcut, Insider threats in Cyber Security: The enemy within the gates**, arXiv preprint arXiv:1911.09575, 2019.

[21] M. Baezner, Iranian **cyber-activities in the context of regional rivalries and international tensions**, ETH Zurich, 2019.

[22] Z. Cekerevac, Z. Dvorak, L. Prigoda, P. Cekerevac, "Internet of things and the man-in-the-middle attacks–security and economic risks", MEST Journal, 5(2), 15-25, 2017.

[23] V. Huovila, **Improving the Security of SQL Server using SQL-Map Tool**, 2024.

[24] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, R. A. Khan, "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications", IEEE Access, 8, 48870-48885, 2020.

[25] E. D. Wolff, K. M. GroWlEy, M. O. Lerner, M. B. Welling, M. G. Gruden, J. Canter, "Navigating the solarwinds supply chain attack", Procurement Law., 56, 3, 2021.

[26] P. D. Witman, S. Mackelprang, "The 2020 Twitter Hack--So Many Lessons to Be Learned", *Journal of Cybersecurity Education, Research and Practice*, 2021(2), 2022.

[27] M. Baezner, P. Robin, **Stuxnet**, No. 4, ETH Zurich, 2017.

[28] A. Papathanasiou, G. Liontos, V. Liagkou, E. Glavas, "Business email compromise (BEC) attacks: threats, vulnerabilities and countermeasures—a perspective on the greek landscape", *Journal of Cybersecurity and Privacy*, 3(3), 610-637, 2023.

[29] J. Ciaccio, I. Onat, **An Analysis of ATM and Point-of-Sale Skimming**, Policy, 2025.

[30] G. Lee, S. Shim, B. Cho, T. Kim, K. Kim, "Fileless cyberattacks: Analysis and classification", *ETRI Journal*, 43(2), 332-343, 2021.

[31] A. Munsch, P. Munsch, "The Future of API Security: The Adoption of APIs for Digital Communications and the Implications for Cyber Security Vulnerabilities", *Journal of International Technology & Information Management*, 29(3), 2020.

[32] T. Russo, **Simulated Trust: How Malicious Actors Take Advantage of Cellular Carriersto Perform SIM Swapping Attacks**, 2019.

[33] N. Kshetri, J. F. DeFranco, J. Voas, "Is it live, or is it deepfake?", Computer, 56(07), 14-16, 2023.

[34] P. Rohmeyer, T. Ben-Zvi, "Managing Cloud Computing risks in financial services institutions", **2015 Portland International Conference on Management of Engineering and Technology (PICMET)**, 519-526, Ağustos 2015.

[35] O. V. Kuzmenko, **Trends of fraud operations on the banking market and approaches of cybersecurity assessment**, 2020.

[36] J. A. Hill, "SWIFT bank heists and article 4A", J. Consumer & Com. L., 22, 25, 2018.

[37] A. Efe, D. Atakan, Ü. G. Altun, "SWIFT attack via phishing against MIS of mobile banking security", *Yönetim Bilişim Sistemleri Dergisi*, 4(2), 24-48, 2019.

[38] F. K. Gündüz, "Kimlik Avı saldırılarının tespitinde sınıflandırma algoritmalarının performans karşılaştırılması", **Bilgisayar Bilimleri Ve Mühendisliğinde Öncü Ve Yenilikçi Çalişmalar**, 129.

[39] Z. Çon, F. Arıca, "Dijital bankacılığın geleceği: Türkiye'deki yenilikler ve küresel trendler", *Girişimcilik ve Kalkınma Dergisi*, 19(2), 21-32, 2024.

[40] E. Dalbudak, Ö. F. Rençber, "Çok kriterli karar verme yöntemleri üzerine literatür incelemesi", *Gaziantep Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 4(1), 1-17, 2022.

[41] F. Ersöz, M. Kabak, "Savunma sanayi uygulamalarinda çok kriterli karar verme yöntemlerinin literatür araştirmasi", *Savunma Bilimleri Dergisi*, 9(1), 97-125, 2010.

[42] E. Güven, M. Pınarbaşı, H. M. Alakaş, T. Eren, "Doğal Afetlerin Tetiklediği Teknolojik Kazaların Risk Azaltma Kriterlerinin Anp Yöntemiyle Ağırlıklandırılması", *Disaster Science and Engineering*, 9(1), 34-42, 2023.

[43] E. Erol, E. Özcan, T. Eren, "Elektrik üretim santrallarında iş güvenliği uzmanı seçiminde hibrit bir karar modeli", *Journal of Turkish Operations Management*, 5(1), 615-629, 2021.

[44] E. Güven, M. Pınarbaşı, H. M. Alakaş, T. Eren, "Evaluation of Natech risk criteria with range valued Neutrosophic AHP", **4th International Conference on Innovative Academic Studies (ICIAS)**, 2024.

[45] B. Uçakcıoğlu, T. Eren, "Analitik hiyerarşi prosesi ve VIKOR yöntemleri ile hava savunma sanayisinde yatırım projesi seçimi", *Harran Üniversitesi Mühendislik Dergisi*, 2(2), 35-53, 2017.

[46] R. Yumuşak, B. Sarımehmet, T. Eren, "Bir mobilya üretim tesisi için üretim geliştirme mühendisi seçimi", *Journal of Turkish Operations Management*, 7(1), 1469-1482, 2023.

[47] E. Ada, H. Çakır, "TOPSIS ve AHP Çok Kriterli Karar Verme Yöntemlerinin Personel Seçim Sürecine Uygulanması", *International Journal of 3D Printing Technologies and Digital Industry*, 6(2), 186-200, 2022.

[48] B. Bayram, T. Eren, "Çok kriterli karar verme yöntemleriyle afet sonrası geçici depo yeri seçimi", *Acil Yardım ve Afet Bilimi Dergisi*, 3(2), 22-30, 2023.

[49] I. Bose, A. C. M. Leung, "Assessing anti-phishing preparedness: a study of online banks in Hong Kong", Decision Support Systems, 45(4), 897-912, 2008.

[50] Internet: H. Hekim, **Oltalama (Phishing) Saldirilari**, http://www.academia.edu/35136881/Oltalama_Phishing_Saldirilari, 2015.

[51] N. Yalçın, A. Avşar, **Sosyal Mühendislik Atakları Ve Alınması Gereken Önlemler.**

[52] M. Alanezi, "Phishing Detection Methods: A Review", Technium, 3(9), 2021.

[53] Y. Arslan, "Oltalama Saldırıları Farkındalık Tatbikatı Örneği", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 9(3), 348-358, 2021.

[54] M. Eren, Bankacılık ödeme Sistemlerinde Siber güvenlik farkındalığı: **Türk bankacılık sektöründe farkındalığın Belirleyicileri üzerine Bir Uygulama, Doktora Tezi**, Marmara Üniversitesi, 2023.

[55] H. Kör, M. Erdoğa, "Oltalama Saldırılarına Yönelık Bır Araştırma", **Onursal Başkan/Honorary Chaırman Prof. Dr. İdris DEMİR**, 228.

[56] A. K. Doing, E. Barbaro, F. van der Roest, P. van Gelder, Y. Zhauniarovich, S. Parkin, "An analysis of phishing reporting activity in a bank", **Proceedings of the 2024 European Symposium on Usable Security,** 44-57, Eylül 2024.

[57] M. Erdoğan, **Siber suçlarla ilgili 2000-2023 yılları arasındaki çalışmaların bibliyometrik analizi, Yüksek Lisans Tezi**, Hitit Üniversitesi, 2024.

[58] P. H. Nguyen, L. A. T. Nguyen, H. A. T. Pham, T. H. T. Nguyen, T. G. Vu, "Assessing cybersecurity risks and prioritizing top strategies In Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number", Heliyon, 10(19), 2024.

[59] N. Z. Yasmin, A. Safira, M. Taupiq, M. S. Oktavia, F. Dhiva, I. Muslim, **Risiko Phishing dalam Transformasi Digital Layanan Perbankan di Indonesia: Evaluasi bagi Bank BUMN.**

[60] S. Yıldırım, "Bankacılıkta Uzaktan Kimlik Tespitinde Karşılaşılan Riskler ve Çözüm Önerileri", **Mülkiye Dergisi**, 48(1), 243-276, 2024.

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

[62] N. N. Cele, S. Kwenda, "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review", Journal of Financial Crime, 32(1), 31-48, 2025.

[63] Internet: **Cozumpark, Phishing nedir? Kimlik avı saldırıları nasıl tanımlanır ve önlenir?**, https://www.cozumpark.com/phishing-nedir-kimlik-avi-saldirilari-nasil-tanimlanir-ve-onlenir/, 28.04.2025.

[64] Internet: **Gaissecurity, PHISHING Hakkında Her şey | Gais Cyber Security,** https://gaissecurity.com/blog/phishing-hakkinda-her-sey/, 28.04.2025.

[65] Internet: **Güney Bilişim, Kimlik avı ve sosyal mühendislik saldırıları: Dijital dünyanın büyük tehlikeleri**, https://www.guneybilisim.com/blog/kimlik-avi-ve-sosyal-muhendislik-saldirilari-dijital-dunyanin-buyuk-tehlikeleri, 28.04.2025.