CUSTOMER AWARENESS AND CYBER SECURITY IN THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT COUNTRIES

Aws AlHares *, Zahra Zaerinajad **, Mohammed Al Bahr **

* *Corresponding author*, College of Business, University of Doha for Science and Technology, Doha, Qatar
Contact details: College of Business, University of Doha for Science and Technology, 24449 Arab League St., Doha, Qatar
** College of Business, University of Doha for Science and Technology, Doha, Qatar

OPEN ACCESS

How to cite this paper: AlHares, A., Zaerinajad, Z., & Al Bahr, M. (2024). Customer awareness and cyber security in the Organisation for Economic Co-operation and Development countries [Special issue]. *Corporate & Business Strategy Review, 5*(1), 371–381.
https://doi.org/10.22495/cbsrv5i1siart11

ISSN Online: 2708-4965
ISSN Print: 2708-9924

Received: 30.03.2023
Accepted: 01.03.2024

JEL Classification: D81, G30, G32, G34, G38, M40, M41, M48
DOI: 10.22495/cbsrv5i1siart11

Abstract

In certain circumstances, millions of documents have been exposed due to an increase in the yearly incidence of cyber security breaches in recent years. In the context of the banking industry's digital transition in the Organisation for Economic Co-operation and Development (OECD), this study investigates consumer knowledge of and satisfaction with cyber security. The study is empirical and based on the data obtained from 240 banking clients in OECD. Cyber attacks, phishing, and hacking have been examined from diverse angles. The effects of cyber attacks, phishing, hacking, cyber security help, and expectations on cyber security's technical awareness are investigated using analysis of variance (ANOVA) and bivariate regression analysis. The findings demonstrate how the banking industry has benefited from digital change, and users gain from online services. Nonetheless, a customer's degree of awareness regarding hacking, phishing, and cyber attacks will have an impact on how satisfied they are with digital transactions. The findings also showed that banks should regularly offer training programs to protect their clients from cyber attacks and that customers need more assurance from banks about security-related issues. Banks might easily meet their long-term sustainability goals if they implemented better safer cyber security management. This paper has repercussions for policymakers, investors, and business organizations. Importantly, our study reveals how customer awareness and cyber security are related in OECD.

Keywords: Customer Awareness, Cyber Security, Marketing Theory, Phishing Attacks

Authors' individual contribution: Conceptualization — A.A. and Z.Z.; Methodology — A.A. and Z.Z.; Validation — Z.Z.; Formal Analysis — A.A. and Z.Z.; Investigation — A.A.; Resources — A.A., Z.Z., and M.A.B.; Data Curation — A.A., Z.Z., and M.A.B.; Writing — Original Draft — A.A. and Z.Z.; Writing — Review & Editing — A.A. and Z.Z.; Supervision — A.A.; Project Administration — Z.Z.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

Although there are many opportunities presented by digital transformation in the banking industry, there are also several problems. Simple methods for carrying out many financial transactions as part of the banking industry's digital transition include mobile banking and online banking. Customers gain from these services, but they also face substantial challenges due to the threat and potential for cyber attacks. The digital revolution of the banking industry has created several important issues, including cyber attacks, financial fraud, hacking, phishing, and security awareness (Sekhar &

Kumar, 2023). Customers' understanding of cyber security may often be more ambiguous in several respects. While utilizing the digital platforms of the banks, they must be aware of safe technological practices.

Clients of the bank are increasingly becoming digital/cyber literate as a result of cyber attacks, phishing, and hacking. The development and innovation of digital technology represent a huge challenge for the banking industry. It has been deemed an opportunity for growth and development in the existing business model of the bank and a danger to the viability of the bank's corporate existence. In this type of digital transformation, information technology is equally crucial. It offers a foundation for significant innovation in digital services and operation support on a variety of technical fronts. Monitoring the bank's cyber security requires extensive discussion. Banks are currently digitizing all financial services as part of the digital transformation, including the private data of their clients that is kept and sent through a network.

Due to the lack of awareness among users of Internet and mobile banking, these services are subject to numerous hacks. To prevent such assaults and improve consumer satisfaction, banks must upgrade their cyber security procedures. Banking consumers need to actively be aware of ATM skimming if they want to protect themselves from this kind of theft. Targeted action is necessary to address the pervasive issue of ATM skimming (Verizon, 2021). When skimming tools, such as the false keypad and rain cover, are put on ATMs, it is referred to as ATM skimming. The already pervasive problem of card fraud in the banking industry is further exacerbated by card skimming.

The digital revolution of banking operations has made cyber security knowledge a crucial factor in securing our mobile banking applications and Internet banking-related activities (Gartner, 2020). The three primary cyber security categories discussed in the paper are phishing, hacking, and cyber attacks. To keep users of online banking and mobile banking applications safe from cyber attacks, it is crucial to investigate and comprehend their degree of cyber security knowledge. Customers will have a better understanding of many general and technical elements of their cyber security thanks to the current study. Also, it will aid banks in understanding the degree to which clients are now satisfied with the security of the bank, the cyber security support provided by the bank, and their expectations for technological support cyber security services.

The main objective of this study is to evaluate how well customers' cyber security awareness is, including cyber attacks, phishing attacks, and hacking. Additionally, we aim to gauge their level of satisfaction, with services related to cyber security.

The rest of the paper is structured as follows. Section 2 discusses the literature review. Section 3 presents the research methodology. Section 4 provides results and discussion. Section 5 provides conclusions and implications.

2. LITERATURE REVIEW

In recent years, the Organisation for Economic Co-operation and Development (OECD) has seen a significant shift towards digital banking services. This digital transformation has made banking more convenient, accessible, and efficient for customers. However, with this shift comes an increased risk of cyber security threats (OECD, 2021). The rise in cybercrime has highlighted the need for customers to be more aware of their cyber security and to take steps to protect themselves from potential threats.

Marketing theory is a body of knowledge that is concerned with the systematic explanation of marketing phenomena (Kotler & Keller, 2016). The purpose of marketing theory is to provide a comprehensive understanding of consumer behavior and the market environment and to inform the development of effective marketing strategies (Fill, 2002). One of the earliest and most influential marketing theories is the consumer decision-making process theory, first proposed by Howard and Sheth (1969). This theory explains the steps that consumers go through when making a purchase, including problem recognition, information search, evaluation of alternatives, and purchase decisions (Howard & Sheth, 1969). The consumer decision-making process theory is widely used by marketers to understand and influence consumer behavior (Kotler & Keller, 2016).

Another important marketing theory is the theory of market segmentation, which was first introduced by Wendell R. Smith in 1956. This theory explains how organizations can divide the market into smaller groups of consumers with similar needs or characteristics, in order to better target their marketing efforts (Smith, 1956). Market segmentation has become an essential tool for organizations looking to optimize their marketing strategies, and has been widely studied and applied in practice (Fill, 2002).

In addition to consumer behavior and market segmentation theories, marketing theory also includes a number of theories that focus on the psychological and social factors that influence consumer behavior. For example, social identity theory (Tajfel & Turner, 2004) explains how consumers form their self-concept based on the groups they belong to, and how this affects their purchasing behavior. Another example is the theory of consumer motivation, which explains why consumers make certain purchases and how their needs and wants drive their behavior (Maslow, 1943). Marketing theory also includes a number of theories that focus on market structure and performance, including game theory (von Neumann & Morgenstern, 1947) and the structure-conduct-performance paradigm (Scherer, 1990). These theories help to understand the underlying mechanisms of market behavior the impact of market structure on consumer behavior and the success of marketing strategies. Marketing theory is an important tool for understanding the complexities of consumer behavior and the market environment. It provides a comprehensive framework for explaining marketing phenomena and serves as a guide for researchers and practitioners in the development of effective marketing strategies.

Skinner (2019), a renowned psychologist and behaviorist, is known for his work on operant conditioning and the impact of reinforcement on behavior. In recent years, Skinner's theories have been applied to the study of social networks and their role in digitization across various industries (Skinner, 2019). Studies have shown that social

networks have had a profound impact on the process of digitization. They have enabled people to connect and share information with each other in ways that were previously impossible. As a result, they have played a key role in driving innovation and change across industries. One of the key ways in which social networks have impacted digitization is by facilitating the spread of information. Through their ability to connect people from all over the world, social networks have made it easier for ideas and information to spread rapidly. This has had a profound effect on the way in which businesses operate, as companies are now able to access and make use of information from a wider range of sources than ever before (van Dijck, 2013).

A study conducted by the OECD explored customer awareness of cyber security in the era of digital transformation in the banking sector. The study aimed to understand how customers perceive the risks associated with digital banking, what steps they are taking to protect themselves, and what role banks play in educating and protecting their customers from cyber threats. The study found that while customers are generally aware of the risks associated with digital banking, they are not always taking the necessary steps to protect themselves. For example, many customers are using weak passwords, ignoring software updates, and not using two-factor authentication. Additionally, customers are often unaware of the types of scams and phishing attacks that can occur in the digital banking environment. The study also found that banks have a crucial role to play in educating and protecting their customers from cyber security threats. Banks can provide customers with information on how to protect their online accounts, as well as offering tools such as secure browsers and anti-virus software. Banks can also monitor customer accounts for suspicious activity and provide alerts to customers if they detect any potential threats (Sekhar & Kumar, 2023). In conclusion, the study highlights the importance of customer awareness of cyber security in the era of digital transformation in the OECD. Customers need to take steps to protect themselves from potential threats and banks need to play a more proactive role in educating and protecting their customers.

In the rapidly evolving digital landscape of the banking sector within the OECD, the issue of customer awareness regarding cyber security has become a pressing concern for ensuring the safe and successful adoption of digital financial services. With the continuous advancement of technology and the proliferation of digital devices and platforms, cybercrime and cyber attacks are becoming increasingly frequent and severe. These threats pose a significant risk to consumers, businesses, and governments alike, making it imperative that customers are adequately informed and equipped to defend themselves against these potential risks. According to a report by the OECD (2019), the widespread utilization of digital technologies has resulted in an increase in the frequency and severity of cyber security incidents, including both cybercrime and cyber attacks. The report highlights the fact that digital technologies offer numerous opportunities for innovation and growth, but they also present new and complex security challenges. These challenges are particularly prevalent in the banking sector, where sensitive financial information is routinely exchanged and stored electronically. To mitigate these risks, the OECD (2019) places a strong emphasis on the importance of customer awareness and education regarding cyber security. This includes providing customers with information on how to secure their digital devices, such as implementing strong passwords and enabling two-factor authentication. Customers should also be made aware of the dangers of phishing scams and how to recognize and avoid fraudulent activities online. Furthermore, customers should be encouraged to regularly monitor their financial statements and report any suspicious activities to their financial institution.

In addition, the OECD (2020) emphasizes the need for financial institutions to implement robust policies and procedures for responding to cyber security incidents. This includes developing incident response plans that outline the steps that the organization will take in the event of a cyber security breach. Regular risk assessments should also be conducted to ensure that financial institutions are able to effectively identify and manage any potential threats. Financial institutions should also invest in the training and development of their staff to ensure that they are equipped with the necessary knowledge and skills to respond to cyber security incidents. The digital transformation of the banking sector in the OECD is an ongoing process, and customer awareness and education regarding cyber security are critical components of this transformation. As noted by the World Bank (2020), "The establishment of trust in digital financial services is of paramount importance, and this trust can only be achieved through education and awareness" (p. 47). Financial institutions must take a proactive stance in educating customers about the risks and vulnerabilities associated with digital financial services, and empower them with the knowledge and tools necessary to protect themselves. Moreover, financial institutions should be encouraged to adopt a multilayered approach to cyber security, utilizing a combination of technical, operational, and administrative controls to mitigate the risk of cyber security incidents. This can include implementing firewalls, intrusion detection and prevention systems, encryption, and regular software updates. Additionally, financial institutions should also develop and maintain relationships with law enforcement agencies, cyber security consultants, and other stakeholders to ensure a coordinated response to any potential cyber security incidents. In conclusion, customer awareness and education regarding cyber security are crucial components of the digital transformation of the banking sector in the OECD. With the increasing frequency and severity of cyber security incidents, it is imperative that financial institutions take a proactive stance in educating customers about the risks and vulnerabilities associated with digital financial services. Financial institutions must empower customers with the knowledge and tools necessary to protect themselves and establish trust in digital financial services, which is essential for the successful adoption of digital financial services.

With a staggering 30 million Internet users, accounting for 88 percent of its population, Canada stands as another developed nation grappling with significant cyber attacks. Consequently, it has emerged as one of the most cyber security-conscious

countries. Australia, boasting over 20 million Internet users, a substantial student populace, and millions of annual visitors, finds itself in a position where its cyber security regulations impact a vast number of individuals. The nation is actively striving to formulate an impeccable strategy catering to all categories of Internet users. Meanwhile, China leads the world with over 1 billion Internet users, making it the country with the highest online population. As the largest e-commerce corporation globally, the absence of a comprehensive policy could hinder a multitude of individuals from accessing various Internet services (Mishra et al., 2022).

Cyber security is a crucial aspect of digital transformation as it protects an organization's sensitive information and systems from cyber attacks, hacking, and other malicious activities. With the increasing use of technology and digital platforms, the risk of cyber attacks has also risen. Therefore, it is crucial for organizations to prioritize cyber security and implement measures such as firewalls, anti-virus software, and encryption to prevent data breaches and protect sensitive information. Adoption of digital transformation has become imperative for organizations to remain competitive and relevant in the fast-paced digital world. The adoption of digital technologies can improve efficiency, enhance customer experience, and increase revenue. However, organizations must also ensure that they have robust cyber security measures in place to protect their digital assets and information.

The financial sector, particularly the banking sector, has seen a significant transformation with the adoption of digital technologies. Digital transformation in the banking sector has led to the creation of digital banking platforms, mobile banking apps, and online financial services. This has not only improved the customer experience but has also reduced operational costs for banks. However, with the increasing use of technology, the risk of cyber attacks on banks has also increased. A data breach in a bank can result in significant financial losses, loss of customer trust, and damage to the bank's reputation. Therefore, it is crucial for banks to adopt robust cyber security measures to protect their digital assets and customer information. Cyber security is a critical aspect of digital transformation, and its importance cannot be overstated. Organizations must prioritize cyber security and implement measures to prevent data breaches and protect sensitive information. The financial sector, particularly the banking sector, has seen significant transformation with the adoption of digital technologies, but they must also prioritize cyber security to protect their digital assets and customer information.

As traditional banks continue to work with FinTech companies, they are becoming increasingly exposed to cyber attacks. This is due to the increasing reliance on digital platforms, cloud-based systems, and connected devices, which have made traditional banks more vulnerable to cyber threats Beltrame et al. (2022). This can result in the loss of sensitive information, financial losses, and damage to the bank's reputation. For example, in 2019, Capital One was the victim of a massive data breach that resulted in the theft of sensitive information from over 100 million customers (Aviv, 2019). The breach was carried out through a misconfigured firewall in the bank's cloud environment, which was created through its partnership with Amazon Web Services. Another example of a traditional bank that has been affected by a cyber attack after working with a FinTech company is JPMorgan Chase. In 2014, the bank suffered a data breach that exposed the sensitive information of 76 million households and 7 million small businesses. The attack was carried out through the bank's collaboration with a FinTech company, which had weaker security measures compared to JPMorgan Chase.

In addition, the integration of new technologies and systems into traditional banking infrastructure increases the risk of cyber attacks. FinTech companies often prioritize speed and innovation over security, which can result in vulnerabilities in the systems that they use to connect with traditional banks (Hundal & Zinakova, 2021). As traditional banks continue to work with FinTech companies, they are becoming more exposed to cyber attacks. This highlights the need for traditional banks to ensure that their cyber security measures are up-to-date and robust, especially when partnering with FinTech companies. It is important for traditional banks to take proactive measures to prevent cyber attacks and protect their customers' sensitive information.

The rise of digital banking has had a significant impact on customer experience and financial performance in the OECD countries. Digital banking has revolutionized the way financial institutions interact with their customers, providing a more convenient, efficient, and personalized customer experience. The growth of digital technologies, including mobile banking and online banking, has enabled financial institutions to reach new customer segments and improve their financial performance through increased efficiency and cost savings. Mobile banking, in particular, has become increasingly popular in the OECD, as customers seek convenient and secure methods of accessing their financial accounts and performing transactions. Mobile banking has made banking services more accessible to customers, allowing them to access their accounts and perform transactions at any time and from any location, improving the customer experience (Deloitte, 2017). The adoption of digital technologies has also led to increased automation of manual processes and reduced operational costs, which has resulted in improved efficiency and cost savings for financial institutions (Deloitte, 2017). In addition to the benefits of digital banking for customers and financial institutions, the implementation of digital technologies has also presented new challenges and risks. The use of digital technologies has increased the potential for fraud and security breaches, and financial institutions must ensure they have the necessary systems and processes in place to protect customer data and prevent financial crime (European Banking Authority [EBA], 2017). Financial institutions must also comply with relevant regulations and laws, such as data privacy and anti-money laundering regulations, to protect their customers and maintain trust in the banking system (EBA, 2017).

Despite the challenges and risks presented by digitalization, the continued growth of digital banking is expected to shape the future of the banking industry in the OECD. The adoption of digital technologies will continue to provide

opportunities for financial institutions to improve customer experience and financial performance while addressing the challenges and risks associated with digitalization. The banking industry in the OECD must be proactive in addressing the challenges and opportunities presented by digitalization, to maintain customer trust and remain competitive in an increasingly digital world. The implementation of digital banking in the OECD has revolutionized the way financial institutions interact with their customers, providing a more convenient, efficient, and personalized customer experience while also improving financial performance. The growth of digital banking has also presented new opportunities and challenges for financial institutions, including the potential for fraud and security breaches, which must be addressed to ensure customer protection and maintain trust in the banking system. The continued evolution of digital technologies is expected to shape the future of the banking industry in the OECD, and financial institutions must be proactive in addressing the challenges and opportunities presented by digitalization.

The term "digitalization" was first created in 2000 to describe the process of converting physical information into digital format (Weber, 2004). This process has been accelerating in recent years, with the widespread adoption of digital technologies such as the Internet, cloud computing, and mobile devices. The impact of digitalization has been profound, transforming many aspects of modern life, including communication, commerce, entertainment, and education (Brynjolfsson & McAfee, 2012). As a result of this rapid technological advancement, organizations must embrace digital technologies to stay competitive (Manyika et al., 2013).

Digital transformation, which refers to the profound change that organizations and society are undergoing as a result of the diffusion of digital technologies, has been described by Rapp (2023) as a process that requires a holistic approach. This approach must consider not only the impact of technology but also the impact on culture and society. One of the main drivers of digital transformation is the rapid pace of technological advancements, which has led to the development of new technologies such as big data analytics, machine learning, and the Internet of Things (IoT) (Cearley et al., 2017). These technologies have enabled organizations to collect and analyze vast amounts of data, enabling them to make more informed decisions and improve their operations (Accenture, 2019). Another important aspect of digital transformation is the changing customer behavior and expectations. With the rise of digital technologies, customers have become more connected, informed, and empowered, and they expect organizations to provide them with fast and personalized services (Nazari & Musilek, 2023).

Due to the vulnerability of the digital banking industry to a range of cyber attacks, security has become a priority. Banks are expected to maintain and upgrade security measures such as virus controls, firewalls, data encryption, two-factor authentication, and continuous monitoring systems (Gartner, 2020). One of the most significant challenges facing the digital banking industry is the increasing sophistication of cyber threats. According to the 2020 data breach investigations report by Verizon (2021), the financial services sector is the second most targeted industry for cyber attacks, accounting for nearly 20% of all data breaches (Verizon, 2021). In recent years, several high-profile cyber attacks have demonstrated the vulnerability of the banking industry to these threats. For example, in 2016, the Bangladesh Central Bank lost $81 million in a cyber attack that exploited vulnerabilities in its systems ("Bangladesh Bank", 2016). In 2019, Capital One suffered a data breach that exposed the personal information of over 100 million customers (Aviv, 2019). The breach was caused by a misconfigured firewall, highlighting the importance of robust security measures. To address these threats, banks must prioritize security and invest in a range of measures to protect their systems and customer data. Some common security measures used by banks include virus controls, firewalls, data encryption, two-factor authentication, and continuous monitoring systems (Gartner, 2020).

Virus controls are used to detect and prevent the spread of malicious software on bank systems (Gartner, 2020). Firewalls act as a barrier between the bank's internal network and the internet, preventing unauthorized access (Gartner, 2020). Data encryption helps to protect sensitive information from being intercepted or read by unauthorized parties (Gartner, 2020). Two-factor authentication provides an additional layer of security, requiring users to provide a password and a secondary form of identification, such as a one-time code sent to a mobile device (Gartner, 2020). Continuous monitoring systems help to detect and respond to potential security threats in real time. These systems use artificial intelligence and machine learning algorithms to analyze large amounts of data and identify patterns that may indicate a cyber attack (Gartner, 2020). The digital banking industry is vulnerable to a range of cyber attacks, and security is a critical priority. Banks must invest in a range of security measures, such as virus controls, firewalls, data encryption, two-factor authentication, and continuous monitoring systems, to ensure the protection of their systems and customer data (Gartner, 2020). The increasing sophistication of cyber threats highlights the importance of continuous security upgrades to stay ahead of potential threats (Verizon, 2021).

The banking industry has undergone significant changes due to the rise of digitalization, however, the increased use of technology has also led to a major challenge — the loss of trust. According to several studies, the trust deficit in the banking industry has become a significant hindrance to its growth and stability. In the study, Hakimi et al. (2024) highlight the growing concern over the security of online transactions and the fear of data breaches. This fear is fueled by the numerous cases of cyber attacks and identity theft that have plagued the banking sector in recent years. The authors argue that digitalization has not only increased the number of potential security threats but also made it easier for hackers to exploit vulnerabilities in the system.

Similarly, a study by Saeed (2023) found that the lack of transparency in digital banking is a major factor in the loss of trust in the banking sector. They argue that digital transactions are not as transparent as traditional transactions, making it difficult for customers to understand how their data is being

used and by whom. This lack of transparency undermines the trust that customers have in their banks and can lead to a loss of confidence in the banking system as a whole. The role of regulatory agencies in rebuilding trust in the banking sector has also been explored in several studies. In their study, Arinze-Emefo and Ibrahim (2023) found that regulatory agencies play a crucial role in rebuilding trust in the banking sector by ensuring the protection of customer data and promoting transparency in the industry. They suggest that regulatory agencies should encourage banks to invest in cyber security measures and provide customers with clear and concise information about their online transactions (Lucchese et al., 2020).

A similar study by Jena (2023) found that regulatory agencies need to adopt a proactive approach to the regulation of digital banking. They argue that by setting standards and guidelines for digital banking practices, regulatory agencies can help rebuild trust in the industry. Additionally, they suggest that regulatory agencies should also encourage banks to invest in cyber security measures and to provide customers with clear and concise information about their online transactions. In conclusion, several studies have found that the loss of trust in the banking sector is a significant hindrance to its growth and stability. The trust deficit is caused by the fear of security threats, lack of transparency in digital transactions, and a lack of proactive regulation by regulatory agencies. To rebuild trust in the banking sector, regulatory agencies need to adopt a proactive approach to regulation and encourage banks to invest in cyber security measures and improve the transparency of their digital transactions.

Zakaria's (2023) research on the correlation between the rise in cybercrime and the financial inclusion of FinTech companies highlights a growing concern in the financial sector. With the rise of FinTech companies, there has been an increase in the number of people who are using digital financial services, making them a prime target for cybercriminals (Zakaria, 2023). One of the main reasons for the rise in cybercrime is the increasing use of digital technologies in the financial sector. As more people use digital financial services, they are exposing themselves to greater security risks, including hacking, phishing, and other scams. The authors suggest that the lack of regulation and standards for the FinTech sector has contributed to the rise in cybercrime, as there is a lack of accountability for security breaches. Another factor contributing to the rise in cybercrime is the growing popularity of mobile devices and the Internet as a means of accessing financial services. As more people use their smartphones and other mobile devices to access financial services, they are exposing themselves to new security risks, including the exposure of sensitive financial information to cyber attacks. This highlights the need for robust security measures that can protect consumers' data and financial information from cyber attacks. In addition to the rise in cybercrime, Zakaria (2023) also notes that the financial inclusion of FinTech companies has led to new financial vulnerabilities. For example, FinTech companies may not have the same level of security as traditional financial institutions, and they may not have the same level of expertise in detecting and responding to cyber attacks. This can result in the exposure of sensitive financial information to cyber attacks and other security risks. To address the rise in cybercrime and the financial inclusion of FinTech companies, Zakaria (2023) suggests the implementation of a comprehensive approach to cyber security in the financial sector. This approach should include the development of new technologies, the implementation of strong security measures, and the strengthening of regulation to ensure that FinTech companies are held accountable for the security of their customer's data.

Cyber security is a significant issue that affects organizations globally, including those belonging to the OECD. These organizations face various challenges that pose a threat to their reputation, intellectual property, and financial stability. The advancements in technology have made the cyber security risks faced by these organizations more complex, sophisticated, and challenging (PricewaterhouseCoopers [PwC], 2018). In this article, we will discuss the frontline issues faced by OECD organizations in terms of cyber security. One of the primary threats faced by OECD organizations is the risk of cyber attacks. Cybercriminals are constantly developing new methods to steal sensitive information and data, making it essential for organizations to be vigilant in protecting their assets (Australian Signals Directorate [ASD], 2020). A report by the ASD revealed that phishing is the most common type of cyber attack, where an attacker sends an email to an employee posing as a trusted source and requesting confidential information (ASD, 2020). These types of attacks are becoming increasingly sophisticated, making them more challenging for organizations to detect.

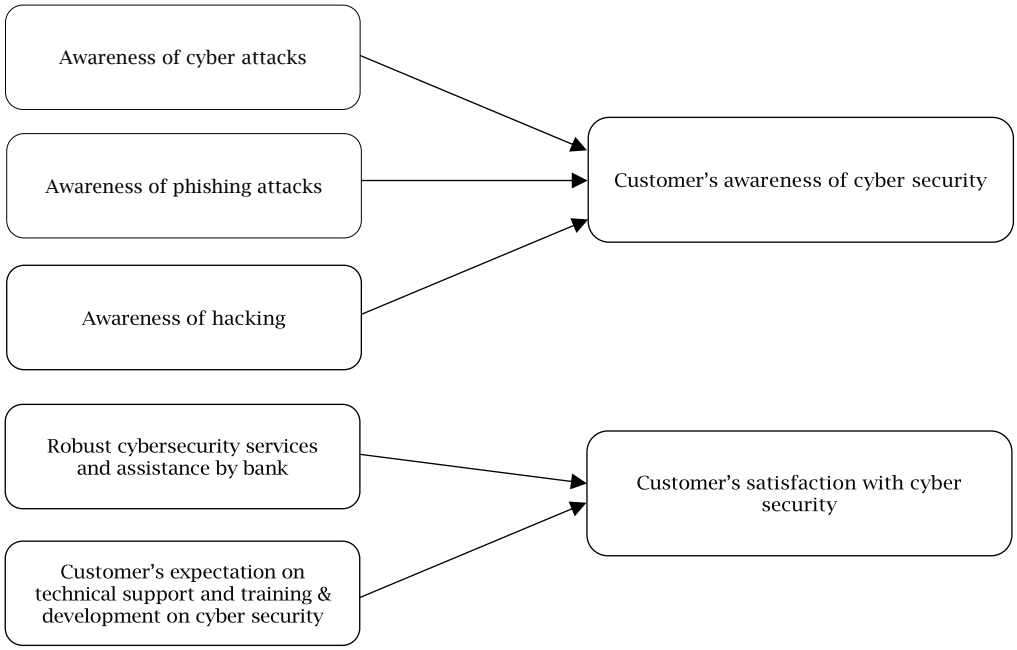
Data breaches are another threat faced by OECD organizations. According to the Global State of Information Security Survey 2018 by PwC, the number of reported data breaches increased by 7% compared to the previous year (PwC, 2018). Data breaches expose confidential information and harm the reputation of the organization, resulting in financial losses. The rise of cloud computing increases the risk of data breaches as it makes it easier for hackers to access sensitive information stored on the cloud. The use of IoT devices has become popular in OECD organizations, but it also introduces new security risks. The lack of standardization in the security of IoT devices makes it challenging for organizations to assess the security of these devices and protect their information (PwC, 2018). IoT devices connected to the Internet are vulnerable to hacking, further increasing the risk of unauthorized access to sensitive information. Ransomware attacks have become increasingly common in recent years and pose a significant threat to OECD organizations. Ransomware is a type of malware that encrypts sensitive data and demands a ransom payment from the organization to unlock it (PwC, 2018). The increasing sophistication of ransomware attacks makes it challenging for organizations to protect their information and prevent the spread of these attacks.

The use of mobile devices in the workplace has also introduced new security risks for OECD organizations. The widespread use of mobile devices makes it easier for employees to access sensitive information on the go, but it also increases the risk of unauthorized access to sensitive information and data breaches (PwC, 2018). Organizations must

ensure that they have robust security measures in place to protect sensitive information stored on mobile devices. To address the critical cyber security threats faced by OECD organizations, it is crucial for organizations to stay informed about the latest trends and developments in cyber security. The OECD provides guidelines and recommendations for organizations to enhance their cyber security measures and promote international cooperation in this area (OECD, 2021). Regular security assessments and audits are necessary to identify potential vulnerabilities and implement appropriate measures to address them. Employee education is also important in reducing the risk of cyber attacks and data breaches. Employees should be trained on how to recognize phishing scams, avoid data breaches, and secure their mobile devices (OECD, 2021). This will help organizations to be better prepared to respond to cyber security threats. The critical cyber security threats faced by OECD organizations are a major concern that requires organizations to be proactive in addressing these threats. Adopting best practices for cyber security, engaging in regular security assessments and audits, and educating employees about the importance of cyber security are crucial steps in ensuring the protection of organizations' information and assets.

This study identified five independent variables: cyber attacks, phishing attacks, hacking, cyber security services and help provided by banks, technical support, cyber security training and development by banks, and advice from a cyber security expert based on an analysis of the literature review. The study identified two dependent variables — consumer knowledge of cyber security and customer satisfaction with cyber security — to better understand the effects of these factors. These variables served as the foundation for the suggested hypothesis and the proposed research model, which aimed to measure the study's aims.

Figure 1. Conceptual framework on customer's awareness of cyber security and conceptual framework on customer's satisfaction with cyber security



Source: Authors' elaboration.

The hypotheses below are being tested following the study's stated goals and proposed model:

H1: There is a relationship between Customer's awareness of cyber security and customer's awareness of cyber attacks.

H2: There is a relationship between customer's awareness of cyber security and customer's awareness of phishing attacks.

H3: There is a relationship between customer's awareness of cyber security and customers' awareness of hacking of mobile apps and Internet banking activities.

H4: There is an effect between robust cyber security services and assistance offered by banks and customers' satisfaction.

H5: There is an effect between technical support and training and development on cyber security by banks and customers' satisfaction.

3. RESEARCH METHODOLOGY

This study employed a quantitative and descriptive research design. Data from both primary and secondary sources were used in the study. Structured questionnaires are considered primary sources. Research papers, journals, business magazines, and published books are examples of secondary sources. The information was gathered from the respondents using a structured questionnaire that was developed with the aid of the literature that was accessible. We asked 30 questions about users' knowledge of hacking, phishing, and other online threats and how they are often affected by them. A thorough literature research was done in order to create the survey questions. To investigate potential literature relevant to the current investigation, the previously published papers were carefully read and evaluated.

The statement-based items that were included in our questionnaire were developed using the literature. When creating the questionnaire's questions, we also looked at the cyber security experts' YouTube video and their comments. This method led to the 30 questions that were utilized in the survey questionnaire. The questionnaire was also pretested on 40 participants, and following a successful test, the final questionnaire was distributed for data collection. The information was gathered using convenience random sampling, a nonprobability sampling technique. The study also included questions about clients' expectations for technical help as well as their satisfaction with the banks' cyber security assistance. A five-point Likert scale was used to evaluate the replies, with 5 — being a strong agreement and 1 — a strong disagreement. The convenience sample approach was used to collect the data. The questionnaire was filled out by 240 participants, who then submitted their answers.

Statistical Package for the Social Sciences (SPSS) was used to examine the information acquired for this investigation. The data that were gathered were examined using the proper statistical methods. The demographic characteristics of the respondents were described using frequencies and percentages using descriptive statistics. Correlation analysis was used to look at how the variables related to one another. Regression analysis and analysis of variance (ANOVA) were used to examine the hypotheses. The analysis of the study is split into two parts. The first component looked at the customer's knowledge of hacking, phishing, and online assaults. The customer's satisfaction with the bank's technological support, cyber security awareness training, and development was analysed in the second segment.

Our analysis consists of two parts. Initially, we examined the extent to which customers are aware of phishing, hacking, and cyber attacks. Subsequently, we assessed customer satisfaction regarding the bank's assistance with cyber security awareness, support, and training programs for cyber security awareness and overall development, in this field.

Table 1 shows the basic stats of key variables by checking out the average, standard deviation, and smallest and largest values. It is clear that all three variables matter a lot for how customers understand cyber security. But, hacking really stands out. It seems to affect customers more than phishing and other types of cyber attacks.

The demographic characteristics of the respondents were analysed. Out of the 240 participants, 140 (58.33%) were males and 100 (41.67%) were females. Regarding age distribution 20 (8.33%) respondents were, below the age of 25 while 120 (50%) fell between the ages of 25 and 45. Additionally, there were 60 (25%) respondents in the age group of 45 to 55 followed by 37 (15.41%) in the age group of 55 to 65, and only three (1.25%) who were over the age of 65. Furthermore, when it comes to background among those surveyed, 60 (25%) had a diploma, 100 (41.66%) held a bachelor's degree, 70 (29.16%) possessed a master's degree, and finally, 10 (4.16%) had obtained a Ph.D. In terms of employment status half of the respondents, 122 individuals 50 (83%) were self-employed whereas slightly less than half 118 individuals 49 (16%) worked for government organizations. Regarding banking preferences, out of all participants surveyed, 220 individuals 91 (66%) had bank accounts conversely 20 individuals 8 (33%) did not possess bank accounts it is noteworthy that an analysis revealed that many respondents favoured banking and internet banking on laptops and desktops for their transactions. This information proves to be valuable for analysis purposes. Table 1 provides statistics including mean values, standard deviations, as well as minimum and maximum values.

4. RESULTS AND DISCUSSION

Investigating and examining the customer's knowledge of cyber security in mobile banking applications and online banking is the major goal of this study. The research analyses the customer's awareness of cyber attacks, phishing, and hacking. The survey also aims to determine how satisfied customers are with the cyber security services supplied by banks, as well as how satisfied they are with the technical assistance and cyber security awareness programs that banks offer. There are two sections to the research. The customer's understanding of cyber security was examined in the first section, with a particular emphasis on hacking, phishing, and cyber attacks. The customer's satisfaction with the cyber security support and the customer's expectations of the bank with regard to cyber security were both examined in the second section of the research. Due to the banking sector's weak defensive mechanism, it is strongly advised to increase knowledge of cybercrime prevention methods. The findings of the ANOVA demonstrated that consumers are aware of cyber attacks, phishing assaults, and hacking, but the level of awareness is not the same in all three types of attacks. The public is more aware of hacking and cyber attacks than phishing.

Table 1. Descriptive statistics of the variables

Variables	*N*	*Minimum*	*Maximum*	*Mean*	*Std. Dev.*
Cyber attacks	240	1.31	5	3.311	0.621
Phishing	240	1.31	5	3.333	0.625
Hacking	240	1.42	5	3.541	0.577

Source: Authors' calculation.

Customers are satisfied with their awareness of cyber attacks, as shown by the first independent variable, cyber attack, being significant in customer satisfaction. Customers would be more satisfied with digital services if banks raised their knowledge of cyber attacks. Customer happiness is found to be unaffected by the second independent variable, phishing, suggesting that customer satisfaction may be higher if customers are aware of phishing. Its insignificance is caused by the clients' substantially lower understanding of the detection of such emails, phone calls, and SMS that result in phishing assaults. The sample data did not reveal any evidence of phishing assaults, but it does indicate that customers are aware of them. Customer happiness is significantly influenced by the third independent variable, hacking, which suggests that customers are satisfied with their knowledge of hacking. This suggests that as customers become more knowledgeable about facts relating to hacking, they will be better happy with the digital services offered by banks.

Table 2 summarizes the constructions' reliability as well as their interpretations. Cronbach's alpha ranged from 0.776 to 0.899, so we are able to see that the data we collected was stable and trustworthy. With this table, it is safe to say that our research scale is okay and reliable.

Table 3 shows the relationship between the dependent variables and independent variables. Typically, the test results are contrasted using Pearson's correlation coefficient. A correlation coefficient value of less than 0.7 is considered good. There was a significant association among awareness of cyber attacks ($r(240) = 0.46$, $p < 0.05$), awareness of phishing attacks ($r(240) = 0.12$, $p < 0.05$), awareness of hacking ($r(240) = 0.62$, $p < 0.05$), and customer's awareness of cyber security.

Table 2. Reliability of measurements

Constructs	*N*	*Number of alpha*	*Cronbach's consistency*	*Internal items*
Customer's satisfaction	240	5	0.812	Excellent
Cyber attacks	240	6	0.811	Excellent
Phishing	240	5	0.833	Excellent
Hacking	240	5	0.899	Excellent

Source: Authors' calculation.

Table 3. Correlation analysis of the variables

Variables	*Cyber attack*	*Phishing*	*Hacking*	*Customer's satisfaction*	*p-value*
Cyber attack	1				0.02
Phishing	0.4318255116	1			0.03
Hacking	0.78717655	0.567915277	1		0.01
Customer's satisfaction	0.462345482	0.124973252	0.625897813	1	0.00

Source: Authors' calculation.

Table 4. Variation analysis of the variables (ANOVA)

Model	*Variables*	*Sum of squares*	*ANOVA[a] Df*	*Mean square*	*F*	*Sig.*
1	Regression	7.451	1	7.271	16.138	0.001[b]
	Residual	48.125	238	0.485		
	Total	53.687	239			
2	Regression	1.222	1	1.123	2.381	0.123[c]
	Residual	51.678	238	0.551		
	Total	53.5699	239			
3	Regression	14.785	1	13.563	41.237	0.003[d]
	Residual	38.812	238	0.222		
	Total	53.699	239			

Note: a. Dependent variable: Customer's awareness of cyber security; b. Predictors: Constant awareness of cyber attacks; c. Predictors: Constant awareness of phishing attacks; d. Predictors: Constant awareness of hacking.
Source: Authors' calculation.

The bank's first independent variable, cyber security support, is discovered to be important in customer satisfaction in the second portion of the research, suggesting that customers need additional cyber security features from banks to protect them from all kinds of cyber attacks. Customer satisfaction is significantly influenced by the second independent variable, which is the customer's expectation of technical assistance and training and development in cyber security. This suggests that clients require a technical support centre, and banks should constantly monitor customers' smartphones, laptops, and desktop computers that they commonly use for Internet banking and mobile banking apps. Consumers must receive frequent training from banks on how to use the Internet and mobile banking in order to raise their understanding of cyber security. Information security depends on people, procedures, and technology, according to a study on employee hacking. Customers will find the study's findings useful in understanding the significance of various cyber security measures and the distinctions between hacking, phishing, and cyber attacks. Its significance is determined by users' capacity for making information security decisions. Users must be aware of the risks to information security and their security responsibilities. The study will assist them in comprehending the value of cyber security knowledge in order to lessen the likelihood of such assaults. Managing and upgrading devices is crucial for cyber security.

Table 5. Regression model summary[b]

Model R	*R^2*	*Adjusted*	*R^2*	*Std. error of the estimate*	*F change*	*Significance F*
1	0.362[a]	0.111	0.122	0.6518	17.131	0.000
2	0.148[a]	0.023	0.011	0.444	3.155	0.133
3	0.525[a]	0.244	0.247	0.465	43.238	0.000

Note: a. Predictors: constant, awareness of cyber attacks, awareness of phishing attacks, and awareness of hacking; b. Dependent variable: Customer's awareness of cyber security.
Source: Authors' calculation.

Customers will need to become more knowledgeable about numerous technological and user interface-related issues in order to lower their risk of being cyber victims. According to the survey, banks should be aware of how cyber security knowledge affects customer satisfaction and should make serious efforts to raise customer cyber security awareness. The findings also imply that the OECD Monetary Authority, which oversees the banking industry in the OECD, should encourage

banks to host cyber security awareness events and regular training sessions on technical support for customers using mobile banking apps and Internet banking services in order to protect them from potential cyber attacks.

5. CONCLUSION

The current study offers a better framework and a deeper knowledge of many aspects relating to consumer cyber security awareness and its impact on their level of happiness.

This study aims to find the relationships between customers' awareness of cyber security and cyber attacks, phishing attacks, hacking of mobile apps, and Internet banking activities. Also, to find the effect between each of the robust cyber security services, technical support, training and development, and assistance offered by banks and customers' satisfaction.

The study goes deep into theoretical foundations and evidence-based results, but it is not perfect. Like any study, there are limitations in place. The main one is the questionnaire research. With these types of surveys, usually fewer people respond which could affect the accuracy of the study. This one focused on clients from OECD banks and unfortunately won't be applicable to everyone since it's limited to a specific group of people. While this is true, common standards in bank financial management can be found worldwide so we still predict that our findings will still work for other banks. Repeating this study at different banks across the globe will enhance its robustness further.

International replication of this study might yield more insightful viewpoints, even in light of the important insights offered by developed countries. Substantial variations in client satisfaction and earnings can be attributed to cultural conflicts between Western standards and conventional practices in quickly emerging areas. We may deepen our comprehension of the way governments function in many contexts by taking into consideration regional traditions and financial circumstances.

The findings show that consumers are aware of cyber security and that awareness affects how satisfied they are with digital banking services. One indication, phishing, is an inconsequential predictor for the dependent variable, customer happiness, whereas cyber security indicators, cyber attacks, and hacking are strong predictors. The examination of the descriptive statistics reveals that customers are aware of hacking, phishing, and cyber attacks. They require frequent training and development from the bank in addition to technological aid to boost their satisfaction with cyber security.

The findings of the ANOVA showed a variation in the degree of consumer satisfaction with hacking, phishing, and cyber attacks. Furthermore, discovered to be important is the connection between the dependent and independent variables. Phishing has less of an impact on customer satisfaction than cyber attacks and hacking. Also, there is a strong link between the bank's technical support for cyber security and client happiness. Whether consumers are currently aware of their cyber security, educating them about cyber attacks, phishing assaults, and hacking will increase their satisfaction. Customers will be more satisfied with online banking services if a bank holds frequent cyber security awareness events and offers the appropriate technical support training and development.

REFERENCES

1. Accenture. (2019). *The post-digital era is upon us: Are you ready for what's next?* https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/pdf-94/accenture-techvision-2019-exec-summary.pdf
2. Arinze-Emefo, I. C., & Ibrahim, U. A. (2023). Cashless banking and performance of deposit money banks. *Open Journal of Business and Management, 11*(6), 3194–3212. https://doi.org/10.4236/ojbm.2023.116174
3. Australian Signals Directorate (ASD). (2020). *Strategies to mitigate cyber security incidents*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents
4. Aviv, D. (2019, August 6). *Capital One data breach: What you need to know* [Post]. LinkedIn. https://www.linkedin.com/pulse/capital-one-data-breach-what-you-need-know-don-aviv-cpp-psp-pci/
5. Bangladesh bank hackers stole $81 million using swift network. (2016). *The New York Times*.
6. Beltrame, F., Zorzi, G., & Grassetti, L. (2022). The effect of FinTech investments on listed banks: Evidence from an Italian sample. *Risk Governance and Control: Financial Markets & Institutions, 12*(2), 47–55. https://doi.org/10.22495/rgcv12i2p4
7. Brynjolfsson, E., & McAfee, A. (2012). *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy* (58895th ed.). Digital Frontier Press.
8. Cearley, D. W., Burke, B., Searle, S., & Walker, M. J. (2017, October 3). *Top 10 strategic technology trends for 2018*. Gartner, Inc. http://brilliantdude.com/solves/content/GartnerTrends2018.pdf
9. Deloitte. (2017). *Digital banking benchmark: Improving the digital performance*. Deloitte Tax & Consulting. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-digital-banking-benchmark.pdf
10. European Banking Authority (EBA). (2017). *Annual report 2017*. https://shorturl.at/nrFHT
11. Fill, C. (2002). *Marketing communications: Contexts, strategies, and applications* (3rd ed.). Financial Time Prentice Hall. https://cir.nii.ac.jp/crid/1130000794859159936
12. Gartner. (2020, May 5). *Gartner magic quadrant for endpoint protection platforms*. Gartner, Inc. https://www.gartner.com/en/documents/4001307
13. Hakimi, M., Aslamzai, S., Adhi, N., & Hakimi, S. (2024). Digital transformation of Afghanistan banking: Exploring e-banking trends and impacts. *KEUNIS, 12*(1), 90–99. https://jurnal.polines.ac.id/index.php/keunis/article/view/5286/109064

14. Hakimi, T. I., Jaafar, J. A., & Aziz, N. A. A. (2023). What factors influence the usage of mobile banking among digital natives? *Journal of Financial Services Marketing* (28), 763–778. https://doi.org/10.1057/s41264-023-00212-0
15. Howard, J. A., & Sheth, J. N. (1969). The theory of buyer behavior. *Journal of the American Statistical Association 65*(331), 1406–1407. https://doi.org/10.2307/2284311
16. Hundal, S., & Zinakova, T. (2021). Financial technology in the Finnish banking sector and its impact on stakeholders in the wake of COVID-19. *Risk Governance and Control: Financial Markets & Institutions, 11*(1), 8–19. https://doi.org/10.22495/rgcv11i1p1
17. Jena, R. (2023). Factors impacting senior citizens' adoption of e-banking post COVID-19 pandemic: An empirical study from India. *Journal of Risk and Financial Management, 16*(9), Article 380. https://doi.org/10.3390/jrfm16090380
18. Kotler, P., & Keller, K. L. (2016). *Marketing management* (15th ed.). Pearson.
19. Lucchese, M., Di Carlo, F., & Incollingo, A. (2020). Risk relevance and volatility of other comprehensive income in the banking sector: Evidence from European countries. *Corporate Ownership & Control, 17*(3), 187–197. https://doi.org/10.22495/cocv17i3art15
20. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.pdf
21. Maslow, A. H. (1943). A theory of human motivation. *Psychological Review, 50*(4), 370–396. https://doi.org/10.1037/h0054346
22. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120*, Article 102820. https://doi.org/10.1016/j.cose.2022.102820
23. Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. *Algorithms, 16*(4), Article 211. https://doi.org/10.3390/a16040211
24. Organisation for Economic Co-operation and Development (OECD). (2017). *OECD digital economic outlook 2017*. https://www.oecd.org/digital/oecd-digital-economy-outlook-2017-9789264276284-en.htm
25. Organisation for Economic Co-operation and Development (OECD). (2019). *Education at a glance 2019: OECD indicators*. https://doi.org/10.1787/f8d7880d-en
26. Organisation for Economic Co-operation and Development (OECD). (2020). *OECD digital economic outlook 2020.* https://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm
27. Organisation for Economic Co-operation and Development (OECD). (2021). *OECD economic outlook* (Volume 1, Issue 1). https://doi.org/10.1787/edfbca02-en
28. PricewaterhouseCoopers (PwC). (2018, January). *The global state of information security survey 2018.* PricewaterhouseCoopers Risk Services Pte Ltd. https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf
29. Rapp, A. (2023). Human–computer interaction. In *Oxford research encyclopedia of psychology*. https://doi.org/10.1093/acrefore/9780190236557.013.47
30. Saeed, S. (2023). A customer-centric view of e-commerce security and privacy. *Applied Sciences, 13*(2), Article 1020. https://doi.org/10.3390/app13021020
31. Scherer, F. M., & Ross, D. (1990). *Industrial market structure and economic performance* (3rd ed.). Houghton Mifflin Company.
32. Sekhar, C., & Kumar, M. (2023). An overview of cyber security in digital banking sector. *East Asian Journal of Multidisciplinary Research, 2*(1), 43–52. https://doi.org/10.55927/eajmr.v2i1.1671
33. Skinner, B. F. (2019). *The behavior of organisms: An experimental analysis*. BF Skinner Foundation.
34. Smith, W. R. (1956). Product differentiation and market segmentation as alternative marketing strategies. *Journal of marketing, 21*(1), 3–8. https://doi.org/10.1177/002224295602100102
35. Tajfel, H., & Turner, J. C. (2004). The social identity theory of intergroup behavior. In J. T. Jost, & J. Sidanius (Eds.), *Political psychology* (1st ed., pp. 276–293). Psychology Press. https://doi.org/10.4324/9780203505984-16
36. van Dijck, J. (2013). *The culture of connectivity: A critical history of social media.* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199970773.001.0001
37. Verizon. (2021). Verizon: Data breach investigations report 2020. *Computer Fraud & Security*, *2020*(6). https://doi.org/10.1016/S1361-3723(20)30059-2
38. von Neumann, J., & Morgenstern, O. (1947). *Theory of games and economic behavior* (60th ed.). Princeton University Press.
39. Weber, S. (2004). *The success of open source*. Harvard University Press. https://doi.org/10.4159/9780674044999
40. Zakaria, P. (2023). Financial inclusion to digital finance risks: A commentary on financial crimes, money laundering, and fraud. In N. T. Abeba (Ed.), *Financial technologies and defi: A revisit to the digital finance revolution* (pp. 123–130). Springer International Publishing. https://www.springerprofessional.de/en/financial-inclusion-to-digital-finance-risks-a-commentary-on-fin/23871990