

Measuring the Public Awareness of Banking Fraud in Bahrain: A Business Analytics Approach

JOOD MIRZA, RAWAN ALKHAJAH, FATIMA SALEH, AFNAN ALKHABBAZ,
MINWIR AL-SHAMMARI
College of Business Administration
University of Bahrain
Sakhir
BAHRAIN

Abstract: - This research explores clients' awareness of banking fraud at a commercial bank in Bahrain and indicates considerable gaps in understanding various types of fraud. As digital banking becomes increasingly ubiquitous, the risks of online fraud have skyrocketed, posing daunting problems for both customers and financial institutions. The knowledge and experiences of 251 participants—including customers of Bahrain's Commercial Bank and other banks—regarding financial fraud were evaluated. According to the research, only 30.3% of respondents had a moderate understanding of fraud, particularly regarding investment fraud and phishing. Furthermore, 20.7% of respondents reported being victims of fraud, underscoring the urgent need for better consumer education. Although 70.5% of participants reported that their banks had provided information on preventing fraud, the effectiveness of these communications appears inadequate, endangering many people. This study emphasizes the urgent need for improved consumer education initiatives regarding banking security in Bahrain. Among the study's distinctive aspects are its focus on demographic differences in fraud awareness and its comparison of Commercial Bank of Bahrain clients with those of other banks. The findings suggest that targeted training programs could significantly reduce the risk of banking fraud, enhancing everyone's financial security. In the expanding world of digital banking, filling in these knowledge gaps is essential to building resilience and trust.

Key-Words: - Banking fraud, consumer awareness, digital banking, financial education, business analytics, Bahrain.

Received: June 7, 2026. Revised: July 8, 2026. Accepted: August 2, 2026. Published: September 21, 2026.

1 Introduction

The emergence of digital banking, which provides users globally with unparalleled accessibility and ease, has totally changed financial services. Mobile banking and digital payments, which offer significant benefits such as time savings, cost-effectiveness, faster transactions, and user-friendly experiences for clients, businesses, and financial service providers, have made financial services accessible to many individuals [1]. However, this technical improvement has also contributed to increased digital fraud, posing substantial issues for users. As more financial transactions move online, the security of online transactions is at risk, and unscrupulous actors exploit weaknesses through social engineering, malware, and fraud. Since fraudsters are always looking for ways to gain access to financial networks, information system security issues are an inevitable part of this progression [2]. This shift necessitates strengthening safeguards

against online banking fraud for both individuals and financial institutions.

Even as fraud has become more common, many people remain unaware of its various manifestations, leaving them vulnerable to abuse. Although prior research has emphasized the importance of public awareness in reducing these hazards, information gaps remain, especially among specialized groups [3]. Fraud is defined in academic literature as behavior intended to secure an unfair advantage over another by concealing essential information [4]. In the banking context, fraud is often perpetrated by attackers exploiting vulnerabilities in electronic gateways, resulting in financial service denials for customers [2].

This research aims to evaluate customers' awareness of banking fraud at a commercial bank in Bahrain. The study will identify at-risk demographic groups, evaluate familiarity with different forms of fraud, and offer helpful suggestions to improve fraud

awareness by giving a structured questionnaire to bank customers and those of other institutions.

This article's central question is: How well do Bahraini citizens comprehend the dangers of financial fraud, and what factors affect their knowledge of these risks? This study aims to address gaps in the literature and support the development of more effective fraud-prevention strategies. Our goal in conducting this research is to strengthen the entire security framework in Bahrain's banking industry by providing consumers with vital information.

2 Literature Review

2.1 Fraud Typologies

The four basic categories of financial crime are corruption, fraud, theft, and manipulation. While many types of corruption, such as bribery and kickbacks, are mostly institutional problems, the following types are particularly related to banking crimes committed by customers:

- **Payment Fraud:** This includes criminal activities across various payment channels, such as card-present transactions at points of sale (POS) or ATMs, and card-not-present transactions online [4]. The growing popularity of online and mobile payments has contributed to an increase in card-not-present fraud [5], [6].
- **Identity Robbery:** This entails the unauthorized collection of an individual's personal information to commit fraud. To obtain this information, criminals use tactics such as phishing and ATM skimming. Once compromised, these details are often exploited across multiple platforms, making identity robbery particularly damaging [4].
- **Financial Scams:** These encompass a wide array of deceptive practices aimed at defrauding individuals, including phone scams and targeted schemes targeting vulnerable populations, such as older people. The connection between financial scams, identity theft, and account takeovers underscores the need for effective detection methods [1].
- **Account Takeover:** This occurs when a cybercriminal gains access to a customer's online banking credentials, allowing them to steal funds [1]. Account takeover is closely linked to cybersecurity threats, including data breaches and vulnerabilities [7], [8]. Enhanced authentication methods and security practices are crucial for mitigating these risks [9].
- **Remote Attacks:** These aim to interrupt or redirect a system's session without altering the victim's machine. Common types include:

- **Phishing:** Hackers create fake versions of targeted websites to deceive victims into entering their login details [10].
- **Fishing:** This involves direct social engineering, where hackers trick victims into revealing confidential information [11].
- **Smishing:** This form of phishing utilizes SMS to deceive recipients into disclosing sensitive information, capitalizing on users' trust in text messages [12].
- **Vishing:** Voice phishing utilizes voice messages to steal identities and financial resources, with increasingly sophisticated tactics [10].
- **Cloned Voice-Banking Systems:** Hackers replicate legitimate voice-banking systems to appear official, soliciting customer calls to fraudulent numbers [12].
- **Pretexting:** This involves using fictional backstories to manipulate individuals into providing private information, such as claiming to have lost a device to bypass two-factor authentication [11].

2.2 Fraud Awareness Determinants

Online banking fraud poses a serious threat to customers and financial institutions, underscoring the need to understand its complexity. Fraud is characterized as unlawful deception or breach of trust that impacts financial institutions, particularly banks, and is usually driven by financial gain. Cyber threats such as malware and phishing often lead to online banking fraud, although they are typically handled separately [13]. These methods aim to unlawfully obtain funds or personal data, underscoring the need for greater public awareness [14]. Online banking fraud is made more difficult by threats such as malware and identity theft. Fraud is enabled by poor control and weak defenses [8], [15]. Continuous improvement of protective measures is necessary to manage these threats effectively. Additionally, the banking sector monitors both online and card fraud, underscoring the importance of raising public awareness as a key strategy for lowering digital fraud [16].

2.3 Behavioral Responses

Digital banking services have evolved significantly, contributing to the rise of sophisticated fraud methods, including ATM, online bill payment, and card-not-present fraud. Each has unique characteristics that can affect and weaken the performance of the fraud detection algorithm, driven

by differences in device types, transaction volume, and authentication levels [17].

To effectively tackle banking fraud, establishing secure systems that authenticate user identities and authorize transactions is crucial [2]. Many existing solutions react to fraud only after it has happened, which is counterproductive [17]. Preventing unwanted access requires a proactive strategy. With the increased use of mobile devices, which are more susceptible to theft, educating the public on fraud prevention strategies is crucial [10]. Regulatory agencies are actively working to enhance online banking security and build consumer trust through comprehensive identity verification and improved regulations [6].

The primary measures to avoid fraud are as follows [2], [11]:

- **Verify Recipient Information:** To minimize issues, users should thoroughly review information before sending money.
- **Take advantage of AI and machine learning:** Contemporary technology can identify anomalous transaction patterns and notify users of possible fraud.
- **Include Biometric Security:** Account security is significantly enhanced by features such as fingerprint and facial recognition.
- **Use Security Questions:** Knowledge-based identification provides an additional defense against unauthorized access.
- **Utilize SMS Verification Codes:** Interim codes provided to users' mobile handsets can be utilized to verify identities during login attempts.
- **Adopt Dynamic Security Images:** Prevent phishing by giving users the option to select specific images for their login screens.

Data imbalances impact fraud detection, and criminals continually change their fraud methods, creating a dynamic environment that is challenging to address with static, rule-based systems [2], [18].

To address increasing fraud, a mechanism has been introduced to integrate real-time analytics, machine learning, and graph-based anomaly detection, enabling the detection of more complex patterns in unusual transactions and the identification of suspicious devices. Among the most important techniques are the following [1], [19].

- **Device fingerprinting:** This involves identifying the distinctive characteristics of a user's device to detect any unusual access.
- **Behavioral monitoring** involves comparing user activities with typical detection patterns.
- **Blocklisting/Allowlisting Systems:** Devices are classified based on risk scores.
- **Comprehensive and Differential Analysis:** Evaluating activities across different devices to detect fraud rings.

2.4 Institutional Communication

E-banking fraud has become one of the most lucrative forms of cybercrime today [20]. The growing complexity of these attacks makes detection and preventive strategies more difficult, which encourages the growth of fraudulent activities. Such illicit transactions impose a significant financial burden on both service providers and clients, who risk suffering losses due to negligence. Educating clients is essential to help them evade fraudulent schemes, and a shift toward co-liability should enhance client relationships [21]. Key factors influencing client relations include perceived risk, e-security, trustworthiness, and privacy concerns regarding online transactions [10], [22]. In an era of increasing digitalization, the perceived dangers of cybercrime have become more salient, as clients face potential losses from fraudulent transactions and misuse of personal data [12].

Financial institutions have a unique opportunity to strengthen their relationships with stakeholders and customers thanks to the internet. It can provide crucial information on topics such as fraud prevention and dispel misconceptions. Studies show that fraud-prevention tools are frequently inadequate, especially in developing nations, despite the growing recognition of the importance of proactive online communication. Studies also underline the need to leverage websites alongside traditional media to convey fraud-prevention and risk-management techniques to both staff and clients. Trust, contentment, and a cooperative approach to risk management are the cornerstones of strong customer relationships [23].

The expanded functionality of e-banking transactions enables clients to overcome the hurdles provided by a fragmented media ecosystem. Engaging clients through proactive communication and knowledge management (KM) is essential. These communications should not only educate clients about typical fraud schemes but also provide reassurance. The internet can either spread

misinformation or enable the rapid dissemination of vital knowledge. KM theory is crucial for developing effective fraud-detection messages, highlighting the importance of various types of knowledge [24].

A conceptual framework, whether presented visually or described in detail, outlines the primary constructs and variables to be examined, along with their relationships. A framework for assessing e-banking fraud prevention focuses on three KM dimensions to support proactive client engagement. Knowledge acquisition involves providing clients with tutorial information about websites when new fraudulent activities emerge and reminding them of known cybercrime tactics. Three key message categories should be created: fundamental information about fraud, updated insights, and new alerts. These communications should inform clients about what to expect and how to respond to suspicious circumstances [24].

3 Methodology

This study employs a quantitative, cross-sectional approach to assess clients' knowledge of banking fraud at a commercial bank in Bahrain (Appendix). The study combines primary data collected through an online survey with secondary demographic data from government sources, such as the Bahrain Open Data Portal [25], to explain the findings. The purpose of this study is to assess awareness levels, individual experiences of fraud, and behavioral patterns related to fraud prevention, comparing various demographic groups and commercial bank customers with other bank customers.

The data was analyzed; trends were identified using descriptive and analytical statistics, and outcomes were effectively and clearly visualized using dashboards. High ethical standards are upheld throughout the study design, ensuring anonymity, privacy, and voluntary participation at all times.

4 Results

To gather primary data on Bahraini public awareness, experiences, and perceptions of banking fraud, this study employed a structured, self-administered online questionnaire. Using Google Forms, 251 valid questionnaires were distributed; only 189 were returned. The survey was distributed via direct messaging applications and social media.

Purposive and snowball sampling were two non-probability sampling techniques utilized in the study to gather data. A Google Forms survey link was distributed via WhatsApp for purposive sampling. In

the snowball sampling method, participants were encouraged to recruit friends to participate in the study. To assess the findings, accuracy and environmental relevance were ensured by obtaining official population data from the Bahrain Open Data Portal [25] and using them as a standard for demographic comparisons.

4.1 Demographic Profile of Respondents

There were 37.5% female (n = 94) and 62.5% male (n = 157) respondents in the survey sample. Male respondents outnumbered female respondents by approximately 10 percentage points. Compared with Bahrain's national gender distribution, where males account for 52.03% of the population and females for 47.97% (Figure 1).

By Age, respondents in the 35–44 age range made up the largest group (23.5%), followed by those in the 18–24 (21.1%) and 25–34 (19.1%) age groups. Respondents aged 35 and older were somewhat overrepresented relative to national statistics, suggesting that the largest age groups are 25–34 and 18–24. The oldest and youngest categories were underrepresented; however, more than half are employed (Figures 2 and 3).

The sample employment distribution was balanced across active and inactive economic groups: 53.8% of participants were employed, 23.1% were students, and 23.1% were retired. Further comparison of awareness and perception levels between the commercial bank and other bank customers was possible because 30.3% of respondents (n = 76) identified as current customers (Figure 3).

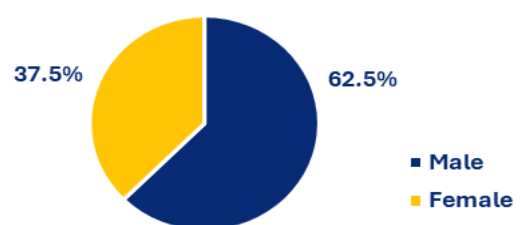


Fig. 1: Gender

Source: Created by the authors

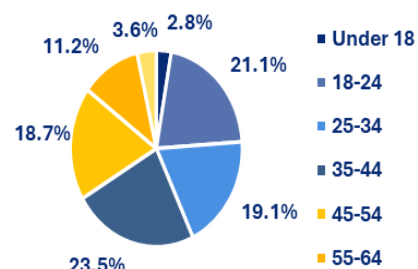


Fig. 2: Age

Source: Created by the authors

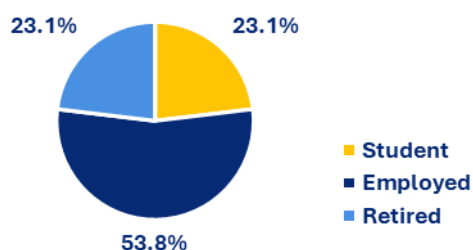


Fig. 3: Employment Status
Source: Created by the authors

4.2 Awareness and Experience with Banking Fraud

Respondents were asked to rate their knowledge of banking fraud. 35.9% reported being quite familiar, 51% reported being familiar, and 13.1% reported being completely unfamiliar. 78.5% of respondents reported experiencing phishing emails or texts, making it the most commonly reported form of fraud. Phone scams followed this step in 71.7% of cases (Figure 4).

Nearly half (48.6%) of respondents said they had experienced investment fraud, while online banking fraud was the next-biggest concern, affecting 59.8% of respondents. The fact that fewer participants knew about identity theft (47.4%), ATM skimming (41.8%), and card cloning (41%) suggests that, while some types of fraud are well known, awareness varies by category, and respondents may choose more than one (Figure 5).

Regarding exposure to fraud, 30.3% reported falling victim to bank-related fraud. The majority of these were categorized as "Unauthorized transactions" (46.1%), with identity theft (28.9%), phishing schemes (21.2%), and others (22.4%) following closely behind (Figure 6).

Surprisingly, no responder mentioned scams as the type of fraud they had experienced. This outcome can indicate a lack of technical know-how or a more constrained public comprehension of fraud.

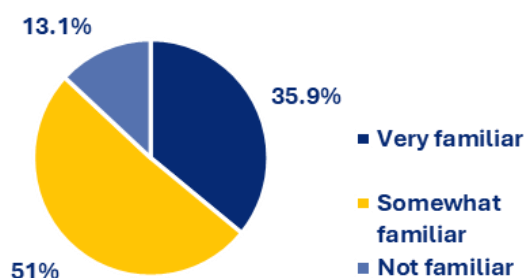


Fig. 4: Familiarity with banking fraud
Source: Created by the authors

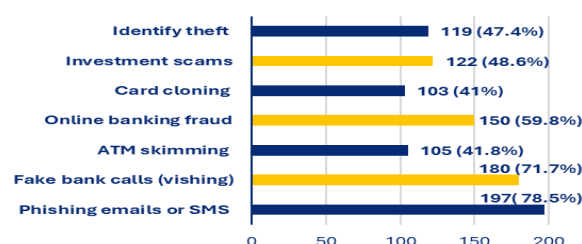


Fig. 5: Awareness of Types of Fraud
Source: Created by the authors

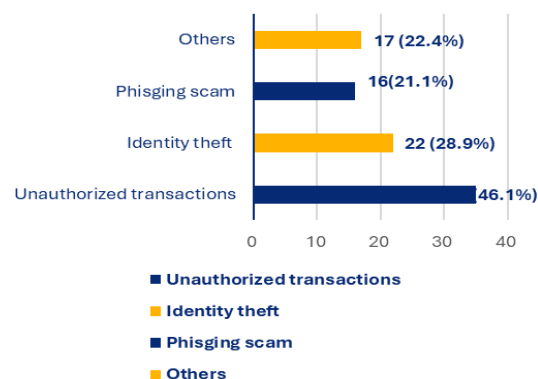


Fig. 6: Individual fraud exposure
Source: Created by the authors

4.3 Fraud Prevention and Bank Communication

Two-factor authentication (2FA) is used by about 59.4% of people for online banking, compared to roughly 1 in 5 (19.9%) who do not use it at all and 20.7% who are unsure. This result suggests confusion about basic banking security practices (Figure 7).

When it comes to updating passwords, the numbers are even more concerning. Just 4% of respondents said they changed their internet banking passwords monthly, 9.2% every 3 to 6 months, and 25.1% once a year. Remarkably, 61.8% of respondents reported never changing their banking passwords, indicating a severe lack of safe online practices (Figure 8).

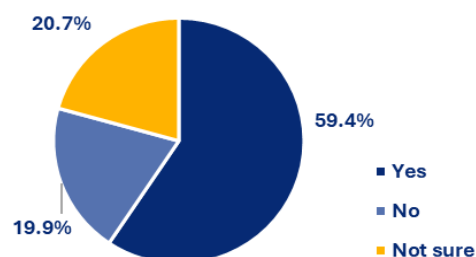


Fig. 7: 2FA Usage of online banking
Source: Created by the authors

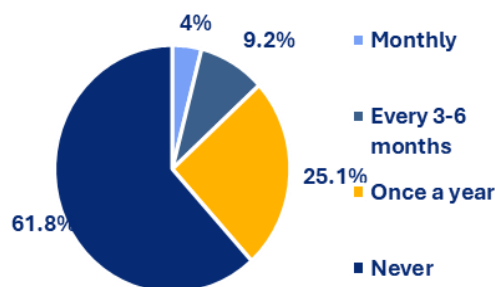


Fig. 8: Frequency of online banking password changes

Source: Created by the authors

Regarding institutional fraud education initiatives, 50.6% of respondents reported receiving explicit fraud-prevention guidelines from their banks (Figure 9), while 70.5% reported receiving fraud-awareness messaging (Figure 10). Satisfaction with their efforts, however, differed. The fraud education provided by their bank was deemed "absolutely effective" by 7.6% of respondents, "moderately effective" by 34.3%, and "unsatisfactory" or "undecided" by the remainder. These findings suggest that while communication is taking place, its impact and efficacy may not be sufficient to change behavior. Of the respondents, 34.3% felt it was "moderately effective," while the remainder were either perplexed or less satisfied (Figure 11).

Among the commercial bank customers, 57.7% expressed trust in the bank's fraud protection systems, 7.7% distrust, and 34.6% remained uncertain. Although commercial bank clients demonstrated marginally higher engagement in fraud prevention behaviors, their perception of the bank's educational effectiveness did not differ significantly from that of other institutions (Figure 12).

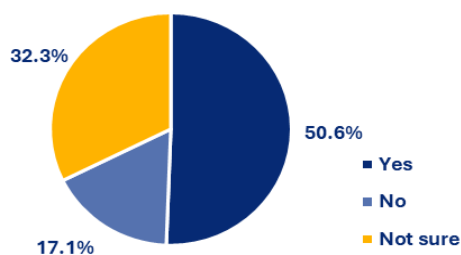


Fig. 9: Satisfaction with banks fraud prevention Guidance

Source: Created by the authors

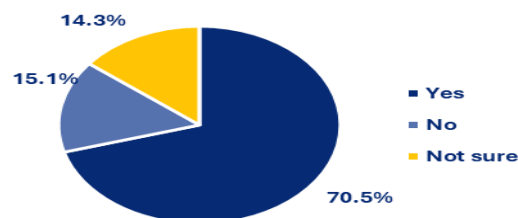


Fig. 10: Received fraud awareness messages from bank

Source: Created by the authors

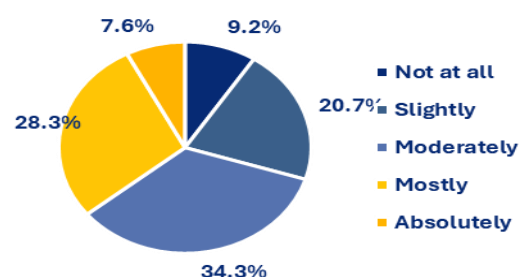


Fig. 11: Perception of banks efforts in fraud education in Bahrain

Source: Created by the authors

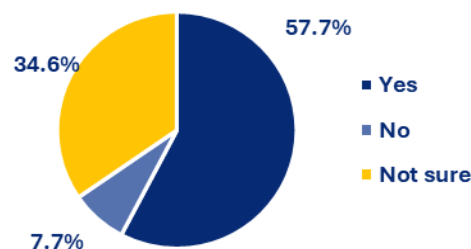


Fig. 12: Fraud prevention guidance from the commercial bank customers

Source: Created by the authors

4.4 Integration with Secondary Data

The study used national statistics from the Bahrain Open Statistics Portal to assess the sample's representativeness and to provide a basis for analyzing demographic realities. As previously stated, although men constitute 52.03% of Bahrain's population (Figure 13), they accounted for 62.5% of the sample. Similarly, only 37.5% of poll respondents are female (Figure 1), although women constitute 47.97% of the country's population. Comparisons of age distributions also showed that, although they are significant in the national profile, the 25–34 and 18–24 age groups are underrepresented. The dashboard containing all the

information gathered from responders is shown in Figure 14.

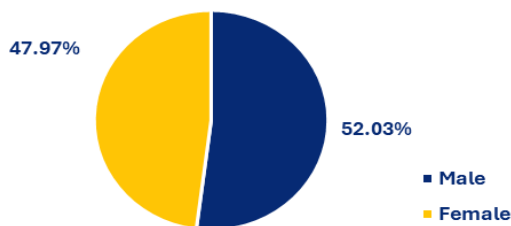


Fig. 13: Bahrain population
Source: Created by the authors

4.5 Spearman Correlation Test

Although the dashboard of collected data is shown in Figure 14, additional analytical results are presented in Table 1 (Appendix), obtained using the Spearman correlation test.

Table 1 (Appendix) correlates the demographic predictors of Age, Gender, and Employment Status with all criterion variables using Spearman rank correlations, which are appropriate for ordinal/binary survey data. Spearman's rank correlations were computed pairwise with listwise deletion per pair. Predictors (Age 1–7, Gender 1–2, Employment 1–3) are regarded as ordinal codes. Cells show (p-value, N) after ρ with significant stars. * $p < .05$, ** $p < .01$, and *** $p < .001$. The pairwise N, corresponding p-values, and ρ with significance stars are shown in the table. Predictors were handled like ordinal codes: Gender (1–2), Age (1–7), and Employment (1–3). Criterion variables included Customer status, trust & guidance, Action frequency, reported fraud, familiarity, received messages, Perceived education, Victim status, General bank guidance, Password change frequency, and 2FA usage

Gender shows small but statistically significant negative associations with use of 2FA ($\rho \approx -0.261$, $p < .001$) and received messages ($\rho \approx -0.128$, $p < .05$), and with familiarity ($\rho \approx -0.158$, $p < .05$). Employment status has small positive associations with received messages ($\rho \approx 0.134$, $p < .05$). Age has small positive associations with Received messages and Victim status (both $p < .05$), but effects remain modest in magnitude. Given mixed measurement levels (binary + Likert), these are nonparametric rank associations. For binary outcomes (e.g., 2FA and victim), logistic regression may provide more precise effect estimates.

5 Discussion and Conclusion

The public's understanding of banking fraud in Bahrain is an important and increasingly pertinent

issue that this essay addresses, especially considering the country's rapid digitalization and the proliferation of financial crimes enabled by cyberspace.

In conclusion, 30.3% of respondents from the commercial bank showed moderate awareness of banking fraud, while 20.7% were Bahraini clients. This familiarity is primarily with phishing emails and texts, and roughly half of respondents have encountered investment scams overall, suggesting that banking fraud is increasing and spreading broadly, whether originating with commercial bank customers or other bank users.

Demographic imbalance in the sample can significantly raise awareness levels. Men and women, for instance, frequently use different social networks and media. Because men make up most of the sample, awareness levels may represent male-preferred venues rather than the general population, such as certain financial forums or sports-related advertising. While men-friendly advertising (such as risk-taking and investing vocabulary) may raise perceived awareness among women who could prioritize security or family-oriented financial decisions, it may also understate the gaps among women.

Younger people, who are overrepresented, usually rely on social media and smartphone apps for information. Young adults are frequently exposed to a range of fraud risks, including student loan fraud and internet fraud. Due to the underrepresentation of older people, awareness scores will be skewed toward traditional media (TV, newspapers), thereby concealing shortcomings in digital outreach.

The results showed that unauthorized transactions are the most common type of fraud respondents are aware of, with phishing emails accounting for the highest percentage (78.5%) and vishing (false bank calls) the second highest (71.7%). Consumers are increasingly exposed to evolving online criminal techniques, as less obvious risks such as identity theft, card cloning, and ATM skimming remain undetected.

Regarding fraud prevention, 70.5% of respondents reported receiving fraud awareness messages from their banks, and 50.6% reported receiving specific fraud-prevention guidance. This result suggests that banks, whether commercial or other financial institutions, continually raise awareness and prevent fraud among their clients.

Sixty-eight percent of participants never change their banking passwords, and over forty-one percent are either unaware of or do not use two-

factor authentication. These behaviors demonstrate fundamental behavioral and cognitive deficiencies.

Regarding clients' trust in the commercial banking system, 57.7% reported trusting the bank's fraud protection measures, 7.7% reported not trusting them, and 34.6% reported uncertainty. This score indicates significant uncertainty and a lack of awareness or confidence; this group is not inherently bad, but it does suggest a potential area for development. In conclusion, many people have fallen victim to financial fraud, indicating that this problem is becoming more prevalent and that raising awareness is essential to stopping it.

The Technology Threat Avoidance Theory (TTAT) explains how people choose to protect themselves from technology-related risks, such as malware, phishing, and data breaches. It is based on the notion that when people detect a threat and think they can successfully escape it, they take preventive measures [26].

The Protection Motivation Theory (PMT) also helps explain why customers adopt security measures, such as using strong passwords, enabling two-factor authentication, and avoiding suspicious links [27]. If customers perceive high severity and vulnerability (e.g., financial loss or identity theft), they are more motivated to act. They are more likely to adhere to fraud prevention standards if they perceive security measures as realistic and simple to implement (high response efficacy and self-efficacy, low response cost). On the other hand, low threat perception or high response costs (such as the hassle of multi-factor authentication) lower compliance.

To promote safer behavior, banks can apply PMT principles to awareness programs that highlight the gravity of fraud and the ease of taking preventive measures. By emphasizing the gravity of fraud and the ease of prevention in their awareness programs, banks can enhance risk and coping evaluations. For instance, marketing that emphasizes the financial and psychological effects of fraud while offering straightforward methods for account protection can significantly improve adherence to security procedures.

The study's findings collectively highlight the need across all demographic groups. Reactive techniques are no longer effective in the digital Age, when fraud is becoming complex and prevalent. Financial institutions, such as commercial banks, can reduce fraud frequency, increase client trust, and strengthen long-term digital banking security by implementing these precautions.

To improve fraud prevention outcomes and close the awareness and behavior gap, we suggest

the following strategic recommendations for banks, notably the Commercial Bank:

- Improve campaigns for Customer Education: Start ongoing multi-channel awareness campaigns using SMS, email, mobile applications, and social media.
- To make them credible and emotionally engaging, use anonymous, real-life fraud stories.
- Use visual materials (movies, infographics) suitable for a variety of age groups and reading levels. Use visual content (movies, infographics) suitable for a variety of age groups and reading abilities.
 - Required Workshops on Digital Literacy: Organize virtual and in-person training sessions that emphasize safe online conduct, password hygiene, and various types of fraud.
 - Exercises in Simulated Fraud: Utilize phishing simulation campaigns to assess and educate bank staff and customers. Those who fall for simulated attempts should receive immediate feedback and instructional materials.
- Enhanced default security procedures:
 - All users should be required to utilize two-factor authentication (2FA).
 - Enforce a minimum password change frequency using system prompts.

Future studies must integrate a wider variety of experimental and simulation results, ideally corroborated by computational models. Incorporating comparative tables would significantly improve the clarity and depth of the analysis and discussion of results.

References

- [1] Kurshan, E., Shen, H., and Yu, H. (2020). Financial Crime and Fraud Detection Using Graph Computing: Application Considerations and Outlook. In: *Second International Conference on Transdisciplinary AI (TransAI)*. IEEE, p. 125-130. DOI:[10.1109/TransAI49837.2020.00029](https://doi.org/10.1109/TransAI49837.2020.00029)
- [2] Ali, M., Hussin, N., and Abed, I. (2019). E-Banking Fraud Detection: A Short Review. *International Journal of Innovation, Creativity and Change*, Vol. 6(8), pp. 67–87.
- [3] Kraivanit, T. (2025). Predictors of digital fraud: Evidence from Thailand. *Journal of Risk and Financial Management*, Vol. 18(12), 67. DOI:[10.3390/jrfm18120671](https://doi.org/10.3390/jrfm18120671)

- [4]. Newman, G. and McNally, M. (2005). *Identity Theft Literature Review*. U.S. Department of Justice, <http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf>. Accessed on 25 July 2026.
- [5]. Drennan, J., Previte, J., and Mort, G. (2006). Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users. *Journal of Organizational and End User Computing*, Vol. 18(1), pp. 1-22. DOI: [10.4018/joeuc.2006010101](https://doi.org/10.4018/joeuc.2006010101)
- [6]. Alfonso, G. H., and Suzanne, S. (2008). Crisis Communications Management on the Web: How Internet-Based Technologies are Changing the Way Public Relations Professionals Handle Business Crises. *Journal of Contingencies and Crisis Management*, Vol. 16(3), pp. 143-153. DOI: [10.1111/j.1468-5973.2008.00543.x](https://doi.org/10.1111/j.1468-5973.2008.00543.x)
- [7]. Kurshan, E., and Shen, H. (2020). Graph Computing for Financial Crime and Fraud Detection: Trends, Challenges, and Outlook. *International Journal of Semantic Computing*, Vol. 14(4), pp. 565-589. <https://doi.org/10.48550/arXiv.2103.03227>
- [8]. Gottschalk, P. (2010). Categories of Financial Crime. *Journal of Financial Crime*, Vol. 17(4), pp. 441-458. DOI: [10.1108/13590791011082797](https://doi.org/10.1108/13590791011082797)
- [9]. Deane, S. (2018). *Federal Financial Exploitation: Why it is a Concern, What Regulators are Doing About it, and Looking Ahead*. U.S. Securities and Exchange Commission, Office of the Investor Advocate. <https://www.sec.gov/files/elder-financial-exploitation.pdf>. Accessed on 25 July 2026.
- [10]. U.S. Faster Payments Council (FPC). (2020). *Examining Faster Payments Fraud Prevention*. U.S. Faster Payments Council. <https://fasterpaymentscouncil.org/userfiles/2080/FraudInfoSharingWP.pdf>. Accessed on 25 July 2026.
- [11]. Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, Vol. 3(3-4), pp. 103-117. DOI: [10.1016/j.ijcip.2010.10.002](https://doi.org/10.1016/j.ijcip.2010.10.002)
- [12]. Brar, T., Sharma, D., and Khurmi, D. (2012). Vulnerabilities in E-Banking: A Study of Various Security Aspects in E-Banking. *International Journal of Computing and Business Research*, online. Accessed on 25 July 2026. <https://www.researchmanuscripts.com/i-society2012/6.pdf>
- [13]. Amiri, M., and Hekmat, S. (2021). Banking Fraud: A Customer-Side Overview of Categories and Frameworks of Detection and Prevention. *Journal of Applied Intelligent Systems and Information Sciences*, Vol. 2(2), pp. 58-68. <https://doi.org/10.22034/jaisis.2021.319773>. 1040
- [14]. Bolton, R. J., and Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, 17(3), pp. 235-255. DOI: [10.1214/ss/1042727940](https://doi.org/10.1214/ss/1042727940)
- [15]. Bhasin, M. L. (2016). Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country. *International Business Management*, Vol. 10(4), pp. 479-492. DOI: [10.3923/ibm.2016.479.492](https://doi.org/10.3923/ibm.2016.479.492)
- [16]. Krambia-Kapardis, M. (2016). *Fraud, Corruption and Financial Crimes: A Handbook for Auditors and Investigators* (2nd ed.). Palgrave Macmillan, ISBN: 9781137406422.
- [17]. Woods, D., and Walter, L. (2022). Reviewing Estimates of Cybercrime Victimization and Cyber Risk Likelihood. *IEEE European Symposium on Security and Privacy Workshops* (EuroSandPW) At: Genoa, Italy.
- [18]. Isedu, M., and Jeffrey, E. (2021). Inside Abuse: A Threat to Banks' Stability. *The International Journal of Business and Management*, Vol. 9(7), pp. 339-348. <https://doi.org/10.24940/theijbm/2021/v9/i7/BM2107-034>
- [19]. Meulen, N. van der (2013). You've been Warned: Consumer Liability in Internet Banking Fraud. *Computer Law and Security Review*, Vol. 29(6), pp.713-718. DOI: [10.1016/j.clsr.2013.09.007](https://doi.org/10.1016/j.clsr.2013.09.007)
- [20]. Carminati, M., Caron, R., Maggi, F., Epifani, L., and Zanero, S. (2014). Bank Sealer: An Online Banking Fraud Analysis and Decision Support System. *29th IFIP International Information Security Conference (SEC)*, Marrakech, Morocco. pp.380-394. https://doi.org/10.1007/978-3-642-55415-5_32
- [21]. Jansen, J., and Leukfeldt, E. (2015). How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. *2015 Workshop on Socio-Technical Aspects in Security and Trust*, Verona, Italy,

- pp. 24-31.
<https://doi.org/10.1109/STAST.2015.12>
- [22] Andrews, L., and Boyle, M. (2008). Consumers' Accounts of Perceived Risk Online and the Influence of Communication Sources. *Qualitative Market Research: An International Journal*, Vol. 11(1), pp. 59-75.
<https://doi.org/10.1108/13522750810845559>
- [23] Greer, C. F., and Moreland, K. D. (2003). United Airlines' and American Airlines' Online Crisis Communication Following the 11 September Terrorist Attacks. *Public Relations Review*, Vol. 29(4), pp. 427-441.
<https://doi.org/10.1016/j.pubrev.2003.08.005>
- [24] Nonaka, I., and Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press, ISBN: 0195092694
- [25] Bahrain Open Data Portal (2025), <https://www.data.gov.bh>. Accessed on 25 July 2026.
- [26] Liang, H., and Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, Vol. 33(1), pp. 71-90.
<https://doi.org/10.2307/20650279>
- [27] Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology: Interdisciplinary and Applied*, Vol. 91(1), pp. 93-114.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Jood Mirza: Conceptualization, Methodology, Software, Data processing, original draft preparation.

Rawan Alkhaja: Conceptualization, Methodology, Software, Data processing, original draft preparation.

Fatima Saleh: Conceptualization, Methodology, Software, Data processing, original draft preparation.

Afnan Alkhabbaz: Conceptualization, Methodology, Software, Data processing, Original draft preparation.

Minwir Al-Shammari: Conceptualization, Supervision, Reviewing, and Editing of the final draft

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US

APPENDIX

Table 1. Spearman Demographic Correlations with Criterion Variables

Predictor	Trust	Guidance	Actions Frequency	Reported Fraud	Familiarity	Received Messages	Education Enough	Victim	Bank Guidance	Password Change	Use 2FA
Age	-0.057 (p=0.6852, N=53)	-0.025 (p=0.8606, N=53)	0.100 (p=0.4758, N=53)	0.149 (p=0.2063, N=74)	0.056 (p=0.3795, N=252)	0.133* (p=0.0347, N=252)	0.059 (p=0.355, N=252)	0.148* (p=0.02, N=252)	0.061 (p=0.3309, N=252)	0.026 (p=0.6835, N=252)	-0.018 (p=0.7806, N=252)
Gender	-0.088 (p=0.5309, N=53)	0.083 (p=0.5544, N=53)	0.107 (p=0.4436, N=53)	0.114 (p=0.3323, N=74)	-0.158* (p=0.0121, N=252)	-0.128* (p=0.0424, N=252)	0.045 (p=0.4802, N=252)	-0.114 (p=0.0720, N=252)	0.005 (p=0.9322, N=252)	-0.076 (p=0.2322, N=252)	- 0.261** * (p=0.0000, N=252)
Employment Status	0.194 (p=0.1642, N=53)	0.028 (p=0.8419, N=53)	0.171 (p=0.2222, N=53)	0.060 (p=0.6100, N=74)	0.025 (p=0.6983, N=252)	0.134* (p=0.0339, N=252)	0.058 (p=0.3556, N=252)	0.089 (p=0.1580, N=252)	0.048 (p=0.4490, N=252)	-0.051 (p=0.4164, N=252)	-0.060 (p=0.3450, N=252)

Source: Created by the authors.

Appendix: Banking Fraud Awareness Survey

1. Choose your Gender:

- Male (1)
- Female (2)

2. Choose your Age:

- Under 18 (1)
- 18 – 24 (2)
- 25 – 34 (3)
- 35 – 44 (4)
- 45 – 54 (5)
- 55 – 64 (6)
- 65 and above (7)

3. Choose your Employment Status:

- Student (1)
- Employed (2)
- Retired (3)

4. Are you a customer of the Commercial Bank in Bahrain?

- Yes (2)
- No (1)

5. How likely are you to trust the Commercial Bank in Bahrain to protect you from fraud?

- 0 Not at all
- 1
- 2
- 3
- 4
- 5 Completely

6. How often do you take efforts to protect yourself from fraud (e.g., reviewing financial statements, avoiding questionable links or messages)?

- Never (1)

- Rarely (2)
- Sometimes (3)
- Often (4)
- Always (5)

7. Do you believe banks in Bahrain are doing enough to educate clients about fraud?

- Not at all (1)
- Slightly (2)
- Moderately (3)
- Mostly (4)
- Absolutely (5)

8. To what extent do you know about banking fraud?

- Very familiar (2)
- Somewhat familiar (1)
- Not familiar (0)

9. Do you feel the Commercial Bank in Bahrain provides enough fraud prevention guidance?

- Yes (2)
- Not sure (1)
- No (0)

10. Which of these types of fraud are you familiar with? (Click on everything that applies).

- Phishing SMS or emails
- Vishing, or phony bank calls
- ATM scanning/skimming
- Fraud in online banking
- Card cloning
- Investment scams
- Identity theft

11. What kinds of fraud are you aware of? (Check all that apply).

- Yes (2)

- Not sure (1)
- No (0)

12. Have you ever been a victim of bank fraud?

- Yes (2)
- No (1)

13. Do you believe Bahrain's Commercial Bank offers sufficient fraud prevention guidelines?

- Yes (2)
- Not sure (1)
- No (0)

14. How frequently do you update your password for internet banking?

- Monthly (4)
- Every 3-6 months (3)
- Once a year (2)
- Never (1)

15. For your online banking, do you employ two-factor authentication (2FA)?

- Yes (2)
- Not sure (1)
- No (0)