Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

DETERMINANTS OF MULTI-FACTOR AUTHENTICATION ADOPTION AMONG PAKISTANI INTERNET USERS: A SURVEY-BASED STUDY

[1]Muhammad Faseeh Ansari, [2]Asjad Abbas, [3]Hamza Ali, [4]Mohsin Nasir
[1-4]Department of Cyber Security, Air University Multan Campus, Pakistan
[1]233628@students.au.edu.pk, [2]233634@students.au.edu.pk, [3]233620@students.au.edu.pk, [4]233650@students.au.edu.pk

DOI:-

Keywords
Multi-Factor Authentication, Cybersecurity Adoption, Pakistani Internet Users, Security Awareness, Digital Security

Article History
Received: 12 March 2026
Accepted: 10 April 2026
Published: 11 May2026

Corresponding Author: *

Abstract
Multi-factor authentication (MFA) refers to an electronic authentication method that requires the use of more than one key. Despite its effectiveness against cyber threats, the use of MFA is still not widely adopted; the case for Pakistan. This research examines the principal factors influencing the intention of MFA adoption among university students and faculty in Pakistan. Through a structured questionnaire, data was collected from the respondents of the academic institutions. The researchers analyzed six distinct features such as perceived security benefit, perceived ease of use, security awareness, social influence and so on. Using descriptive statistics, reliability testing, and correlation analysis, the data were analyzed. The results show that all five independent variables favorably influence MFA adoption intention. The perceived security advantage and social influence appear to be the most prominent drivers while, the perceived ease of use illustrates the usability challenges users associate with MFA. The research concludes with workable suggestions for educators, service providers, and legislators to promote wider adoption of MFA in Pakistan.

Introduction

The growth of online services in banking, education, shopping, and social networking has revolutionized how individuals manage their identities and personal data. The vast number of digital identities and the volume of digital data produced create multiple challenges in protecting one's digital footprints. Authentication has become the core concept that will pave the way for securing digital identities and digital data. In recent years, the weak nature of single authentication factor, especially password based authentication has been highlighted, with top security experts advocating to implement stronger authentication methods that combine several layers. Multi-factor authentication is one such method, where two or more different independent authentication factors are used to lower risk of data or identity loss.

Background of the Study

The digital world has been changed a lot in the past decade and its growth is visible by considering the number of internet subscribers in Pakistan; Pakistan Telecommunication Authority (2024) stated that it has increased from 124 million. But with this rapid growth the rate of cybercrimes has also grown in the recent years and security agencies have reported a significant increase in a variety of cybercrimes, most often tracking related to phishing and credential theft. These fact shows that needs a more robust authentication trend for Internet users in Pakistan.

Furthermore, traditional password-based authentication increasingly shows vulnerability to advanced cyber-attacks, the literature in the field of cybersecurity indicates that the use of breached passwords result in a significant percentage of breaches in the hacking space, with users that settle for using simple and widely used passwords. In addition, security reports from leading tech firms established the profound effect of MFA in reducing the success rate of automated attacks, as one of the most effective security measure accessible to the average user. Even with such strong reasoning, adoption in developing countries such as Pakistan are much lower than their developed counterparts and is undoubtedly faced by contextual challenges.

In addition, there are various contextual variables in Pakistan that affect users' adoption of technologies. Here we want to highlight some contextual variables such as low digital literacy level, lack of awareness of cyber security issues, data privacy concerns, low acceptance of security technology, and the perceived difficulty of technologies that are used to protect through MFA. Another important contextual variable is the fact that the Mobile Internet is the predominant means of accessing the Internet in Pakistan, which needs attention in regards to designing authentication systems.

Research Gap

Nevertheless, literature on technology adoption has been mostly done in the developed countries and very little empirical work has been carried out in context of Pakistan. Most of the existing literature have explored MFA adoption behavior among the Western and East Asian consumers. Further, very little research has been done on role of trust in service providers which is likely to play a very important role in the context of developing countries where institution hand over the life of its members. This research overcomes these limitations and reports the effect of several factors on MFA adoption intention while exploring some unique features of the Pakistani context.

Research Objectives

This study aims to:

1. Examine the current level of MFA awareness and usage among university students and faculty in Pakistan.

2. Investigate the influence of perceived security benefit, perceived ease of use, security awareness, social influence, and trust in service providers on MFA adoption intention.
3. Provide evidence-based recommendations for promoting wider adoption of multi-factor authentication in the Pakistani context.

Research Questions

Based on the research objectives and the identified gaps in the existing literature, this study seeks to answer the following research questions:

1. What is the current level of MFA awareness and usage among university students and faculty in Pakistan?
2. How do perceived security benefit, perceived ease of use, security awareness, social influence, and trust in service providers influence MFA adoption intention among Pakistani internet users?
3. What evidence-based recommendations can be formulated for promoting wider adoption of multi-factor authentication in the Pakistani context?

Literature Review

The literature on authentication technology adoption spans multiple disciplines, including information security, human-computer interaction, and behavioral science. This section reviews conceptual foundations and empirical evidence relevant to MFA adoption, with particular attention to factors identified as determinants of adoption behavior in diverse cultural and technological contexts.

Multi-Factor Authentication: Concepts and Significance

Multi-factor authentication (MFA) is a way for a user to be granted access to a resource which requires having two or more mechanisms of authentication and login. Common MFA methods include a combination of something a user knows such as a password or personal identification number (PIN), something a user has like a security token or mobile phone, and something a user is such as a biometric characteristic. MFA works on the premise that even with an attacker able to compromise one access token, additional tokens would lead to security protection. Studies on MFA usability have indicated that while users recognize benefits of security with MFA; major barriers to use are convenience and ease of use with a number of groups, especially less experienced by technology users (Colnago et al., 2020).

In addition, the role of MFA in today's cybersecurity landscape should not be underestimated. Credential compromise- via phishing, brute-force attack, or data breach-remains one of the most common vectors of attack. In a thorough usability study, Das et al. (2020) discovered that the primary reason users did not implement safeguard measures was: "lack of awareness about the threats to cyber information." Furthermore, presence of MFA alone does not guarantee safe cyberspace-ag users must first be made aware of the threats looking to exploit cyberspace.

Perceived Security Benefit and Adoption Behavior

Perceived security benefit is the belief that the security feature "actually protects" information, and has been shown to be positively associated with adoption across a number of different contexts. If consumers believe that the additional authentication step provides a real security improvement in terms of reducing the threat of account hijacking, they are more likely to accept the effort involved. Ahamed et al., (2024) investigated biometric authentication in Chinese web users and, among the strongest determinants of adoption intention were perceived security benefits, since consumers not only need to recognize functional capabilities of the technology, but be confident in how it functions. In developing

country contexts where the risks and consequences of cybercrime are not always apparent in the face of everyday life, building this perception will rely on campaigns that create informed awareness.

Perceived Ease of Use and Usability Concerns

However, even when users do understand the security advantages, perceived complexity remains a barrier to adoption. Studies have found that in many cases, usability concerns outweigh security in consumers' purchasing decisions. For example, Al-Rahmi et al. (2018) observed that the proportions of Malaysian university students who did not enable MFA due to the setup procedure being perceived as "confusing or taking too much time/effort" (p.4) was significantly higher than those who either enabled the features or never learned how to. This usability-security dichotomy is noted throughout the information systems literature and reflects a key service-provider dilemma.

Security Awareness and Protective Behavior

Similarly, security awareness involves the user's recognition and cognizance of these threats as well as an understanding of the tools available for protection. Related studies have consistently shown that the higher the user's awareness of a particular threat, the higher the likelihood of her conducting protective behavior. Crossler et al. (2013) have argued that the awareness of a threat does not constitute the adoption of protective behavior unless it is coupled with an understanding of the nature of the threat and the tools available to neutralize that threat. In Pakistan, awareness of information security issues skews heavily towards the young, formally educated segments of the population.

Social Influence on Technology Adoption

Whereas social factors pertains to the extent to which the individual perceives what significant others (peers, family members and other authority figures) believed one to use particular technology. In the context of collectivist society (like the Pakistan), where the voice of friends, family and peer always in the focus of attention and hold significant importance, social influence can work as the other important factor. If the friends, colleagues or institution authorities promote and practice the MFA, others are likely to add in. Therefore, in the context of institutions, the faculty recommendations and security policy plays important role in shaping the student behavior (Venkatesh & Davis, 2000).

Trust in Digital Service Providers

Finally, services providers' trust commonly omitted owing to content analysis, is another neglected dimension of security technology adoption literature especially under development country setting. Users have to feel assured that service providers will not misuse their authentication data. Drawing on the previous research on organizational trust, perceived competence, benevolence and integrity has been depicted as three main dimensions of organizational trust (Mayer et al., 1995). Under Pakistan setting, the infrastructure is perceived low while security of platform is doubted, hence, the trust toward service providers is challenging from lacking of new authentication data sharing. Gao et al (2023) confirmed the institutional trust has assisted in predicting a higher ready to adopt biometric authentication.

Figure 1: Literature Review – MFA Adoption Research: Global Contexts and Key Gaps

Empirical Studies on MFA and Authentication Adoption

There has been extensive empirical research conducted on the issues of authentication technology adoption among different end-users in different environments. To provide a foundation for this research, below is a review of evidence from eleven significant piece of research.

Colnago et al. (2020) surveyed 1,931 participants at a US university and found that inconvenience was the primary barrier to MFA adoption, despite widespread acknowledgment of its security benefits. Their work highlighted the critical role of user experience design in determining whether security features are actively utilized.

Similarly, Das et al. (2020) employed a mixed-methods approach to examine MFA adoption behavior and found that lack of threat awareness significantly impeded uptake, particularly among users who had not personally experienced security incidents. They concluded that experiential factors shape both risk perception and protective behavior.

Furthermore, Reese et al. (2019) conducted a usability study comparing five two-factor authentication methods and found that user preferences varied considerably based on perceived convenience and reliability. Biometric methods were generally preferred over token-based approaches, suggesting that adoption strategies should offer authentication method flexibility.

Gao et al. (2023) examined trust and biometric authentication adoption among Chinese internet users and found that perceived trust in service providers was a significant predictor of adoption intention. Their study highlighted that in high power-distance cultures, institutional endorsement carries particular weight in users' adoption decisions.

Likewise, Al-Rahmi et al. (2022) studied Malaysian university students and found a disconnect between security awareness and actual adoption behavior—respondents were aware of security risks but still hesitated to enable MFA due to complexity concerns. This finding points to the need for simplified onboarding experiences.

Moreover, Vance et al. (2012) investigated information security compliance behavior in organizational settings and found that self-efficacy and habit formation were critical to sustaining security practices over time. Their findings suggest that initial adoption alone is insufficient; users must develop routines around MFA use.

In addition, Crossler et al. (2013) provided a comprehensive review of behavioral information security research, identifying key gaps in the understanding of individual security decision-making. They called for research that examines the interplay between cognitive, social, and contextual factors in shaping security behavior.

Ometov et al. (2018) provided a broad survey of multi-factor authentication technologies and adoption challenges, classifying MFA approaches by factor type and analyzing deployment barriers across consumer and enterprise settings. Their work established a technical baseline for understanding the diversity of MFA implementations.

Similarly, Siadati et al. (2017) examined social engineering attacks against SMS-based two-factor authentication and found that users were often vulnerable to manipulation even when MFA was enabled, emphasizing the importance of security literacy alongside technical deployment.

Wiefling et al. (2019) investigated risk-based authentication as an alternative to conventional MFA and found that users responded positively when authentication demands were proportionate to perceived risk levels, indicating that adaptive authentication approaches may improve both security and user satisfaction.

Stobert and Biddle (2014) studied the password lifecycle and found that users actively develop strategies to manage authentication demands across multiple accounts, often at the expense of security. Their work reinforced the need for authentication solutions that integrate naturally into existing user workflows, a consideration directly applicable to MFA adoption design.

Summary of Research Gaps

Most of these examined empirical literature were carried out in Western or East Asian countries and therefore there is a dearth of research on South Asian user members. Furthermore, most of these studies did not consider the simultaneous impacts of security perceptions, social influences, and institutional trust on adoption behaviors instead consider separate influences. Pakistan's unique context in terms of digital literacy practices, mobile-centric use of internet and socio-cultural collectivism demands a separate, novel empirical efforts. This research would fulfill this need.

Table 1: *Summary of Research Gaps in Existing MFA Adoption Literature*

Gap Area	Existing Literature Focus	Gap Identified
Geographic Focus	Western and East Asian populations	Limited research on South Asian, particularly Pakistani, populations
Analytical Approach	Individual adoption factors studied in isolation	Lack of integrated examination combining security perceptions, social dynamics, and institutional trust
Trust in Service Providers	Minimal attention in developing country contexts	Insufficient understanding of how institutional trust shapes MFA adoption in Pakistan
Contextual Factors	Developed country contexts with high digital literacy	Unique Pakistani context: mobile-first usage, limited digital literacy, socio-cultural collectivism

Conceptual Framework

Based on the literature reviewed above the present study developed a conceptual framework, based on Protection Motivation Theory, Security Behavior Theory and Institutional Trust Theory. The conceptual framework of present study Table-1 identified five independent variables that have direct effects on MFA adoption intention of Pakistani internet-users.

Perceived security benefit refers to customers' perceived cognitive judgement of the security benefits that MFA provides to justify this additional authentication process. Perceived ease of use refers to customers' perceived efforts to learn, adopt and use MFA. Security awareness is customers' level of knowledge about security threats as well as their motivation toward taking security-preserving actions. Social influence refers to the customers' perception that relevant other-important peers, family, colleagues, and institutional authorities-have regarding the use of MFA. Trust in service providers is the customers' perception that institutional agents will securely and transparently manage authentication data across platforms.

These five variables are proposed to have a positive influence on MFA adoption intention collectively. This model has been been designed for context of Pakistan and it assumes that all of these factors may be interpreted or effected differently in developing country like Pakistan based on the socio-cultural, economical and technological environment.

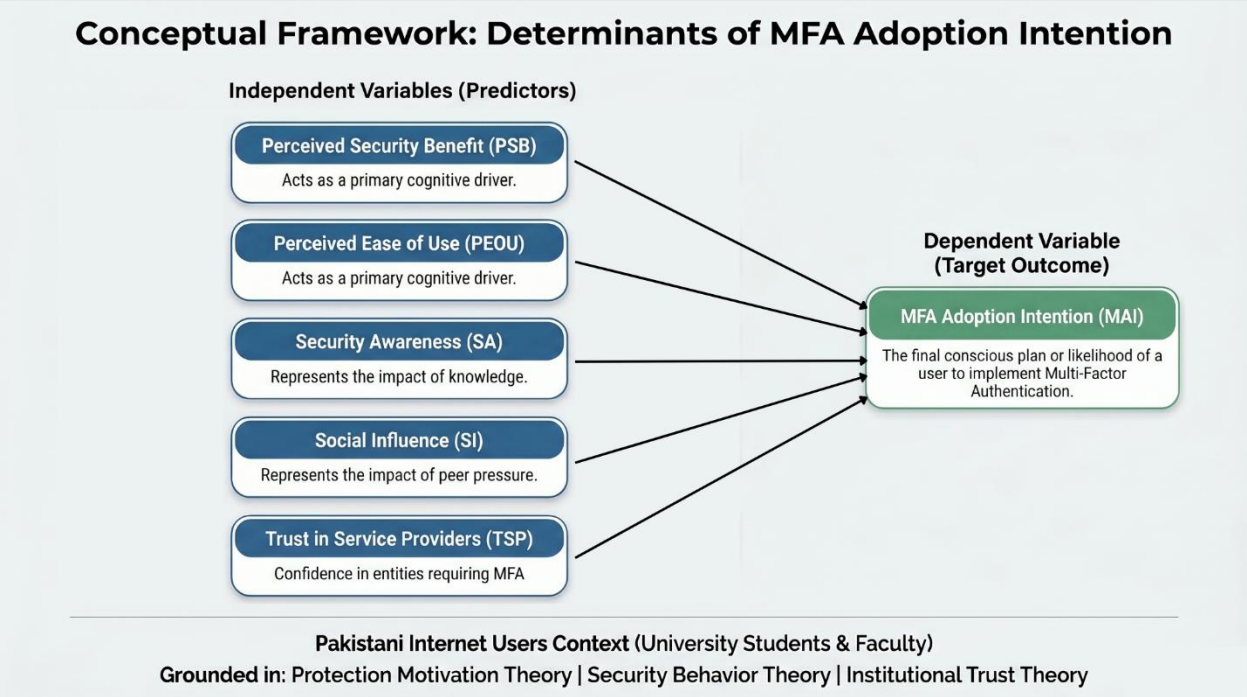

Figure 2: Conceptual Framework – Determinants of MFA Adoption Intention Among Pakistani Internet Users

Material and Methods

Research Design

A quantitative, cross-sectional survey design has been used. This design is appropriate to accomplish a descriptive assessment of the attitudes, perceptions, and behavioral intentions of the selected population at one point in time. Quantitative designs also allow for a systematic study of variables and relationships.

Population and Sampling

The target population consists of undergraduate students, postgraduate students and teaching staff of the universities in Pakistan. It was sampled because it constitutes a technologically active segment of Pakistani internet users who use web-based services such as e-banking, e-learning and social networking sites on a regular basis and generally apply MFA while doing so. A convenience sampling approach was adopted with the sample population sourced from email/online distribution lists and university-based social networking sites and contact points of the researchers in Pakistan. Although the use of convenience sampling diminishes the generalizability of the research findings to the general population, this was a suitable sampling approach for this exploratory investigation given the resource and access limitations.

Sample Size and Data Collection

A total of 100 responses were received. Responses were recorded electronically through Google Form, a free online response system which was chosen for its ease of distribution and the ability to track responses. The list of questions was distributed via the web questionnaire over a four-week period. All responses were anonymous, and respondents were given an informed consent statement to review before completing the web questionnaire.

Research Instrument

A structured questionnaire of 35 items was developed based on a review of validated instruments from prior research on authentication

adoption and cybersecurity behavior. The instrument comprised seven sections: Section A collected demographic information, while Sections B through G contained Likert-scale items measuring the six research constructs. All scale items were rated on a 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). A reverse-coded item was included in the Perceived Ease of Use section to reduce response bias.

Table 1: *Description of Research Instrument*

Variable	Items	Description
Perceived Security Benefit	6	Items measuring users' beliefs about MFA's effectiveness in protecting online accounts
Perceived Ease of Use	6	Items measuring perceived simplicity and convenience of MFA setup and usage
Security Awareness	7	Items measuring knowledge of cybersecurity threats and protective behaviors
Social Influence	5	Items measuring the influence of peers, family, and authority figures on MFA adoption
Trust in Service Providers	6	Items measuring users' confidence in platforms' data handling and security practices
MFA Adoption Intention	5	Items measuring the likelihood and willingness to adopt MFA in the near future
Total	**35**	**Structured Likert-scale items across all research constructs**

Pilot Testing and Instrument Reliability

In addition, the questionnaire was pilot tested on 30 respondents before data collection. Some wording changes were made based on the pilot test to help clarify some items. Once data was collected, reliability was calculated based on Cronbach's alpha. The overall instrument had an alpha of 0.82, which indicates a high internal consistency. The reliabilities by construct range from 0.78 to 0.86 and are well above the recommended minimum of 0.70. All constructs had high reliabilities, indicating that the measurement items accurately represented the construct.

Data Analysis Strategy

The data for all variables were entered and analyzed by IBM SPSS Statistics (Version 26). The data analysis was carried out in three steps. Descriptive statistics (frequencies, percentages, means, standard deviations) were used to describe the demographic variables and all construct variables. Instrument reliability was then tested using Cronbach's alpha. The strength and direction of the relationships was tested between the independent variables and adoption intention for MFA Adoption using Pearson correlations. The results, using narrative description supported by tables and figures, will be described.

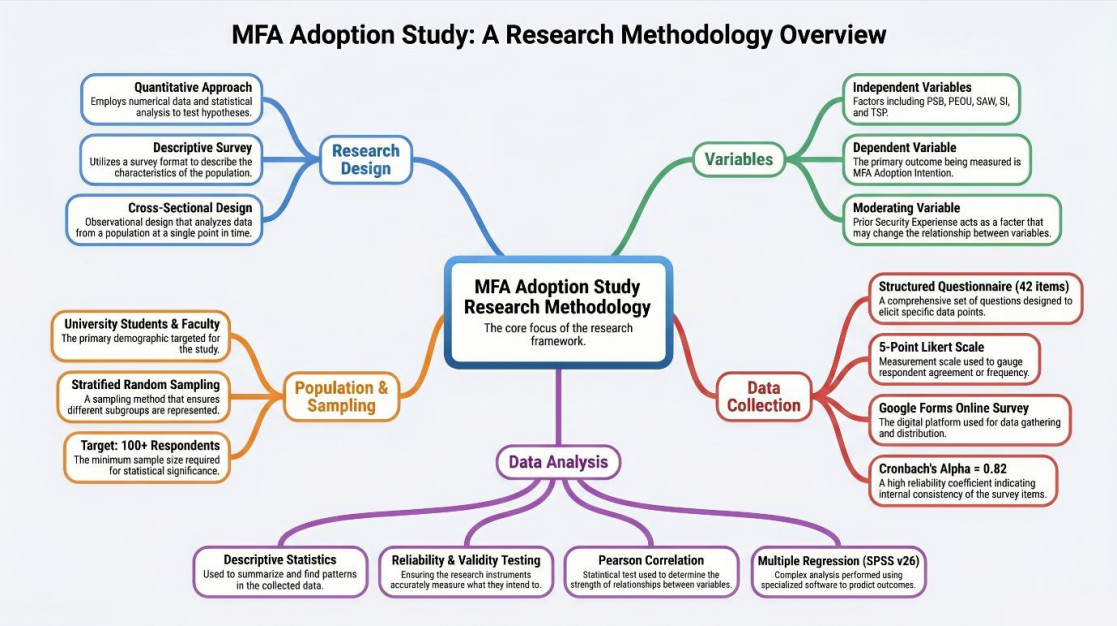

Figure 3: Research Methodology Overview

Data Analysis

Section A: Demographic Profile of Respondents

The demographic information suggests that the sample consisted primarily of young, male, undergraduate respondents -the usual profile of a university based convenience sample at a Pakistani university. The age distribution was heavily concentrated in the 18 to 22 year band, with the 23 to 27 year age group accounting for only a minority of responses, indicating that we were able to characterize the typical undergraduate age group in Pakistan. The gender skew towards male respondents was expected in view of the preponderance of males in Pakistani university-level technological and scientific education. Almost all respondents were studying for a Bachelor's degree.

In addition to the above, the MFA experience data seem to be optimistic as well. Most of the respondents have indicated that they have been using MFA on a regular basis, albeit only a few actually are not using MFA very often. Only a few have used MFA never or did so only once and only one was not even aware of what MFA is. While this unbiased sample arguably does not yet represent the entire Pakistani population online, it does contain a significant number of MFA-experienced users who then constitute the target population of usability and adoption behavior.

Table 2: *Demographic Characteristics of Respondents (N=100)*

Demographic Variable	Category	Frequency	Percentage
Age Group	18–22 years	79	79.0%
	23–27 years	21	21.0%
Gender	Male	73	73.0%
	Female	25	25.0%

Demographic Variable	Category	Frequency	Percentage
	Prefer not to say	2	2.0%
Education Level	Bachelor's	71	71.0%
	Intermediate	27	27.0%
	Matriculation	2	2.0%
MFA Usage Experience	Yes, regularly	66	66.0%
	Yes, but rarely	24	24.0%
	Never used it	7	7.0%
	Tried once, then stopped	2	2.0%
	Not sure what MFA is	1	1.0%

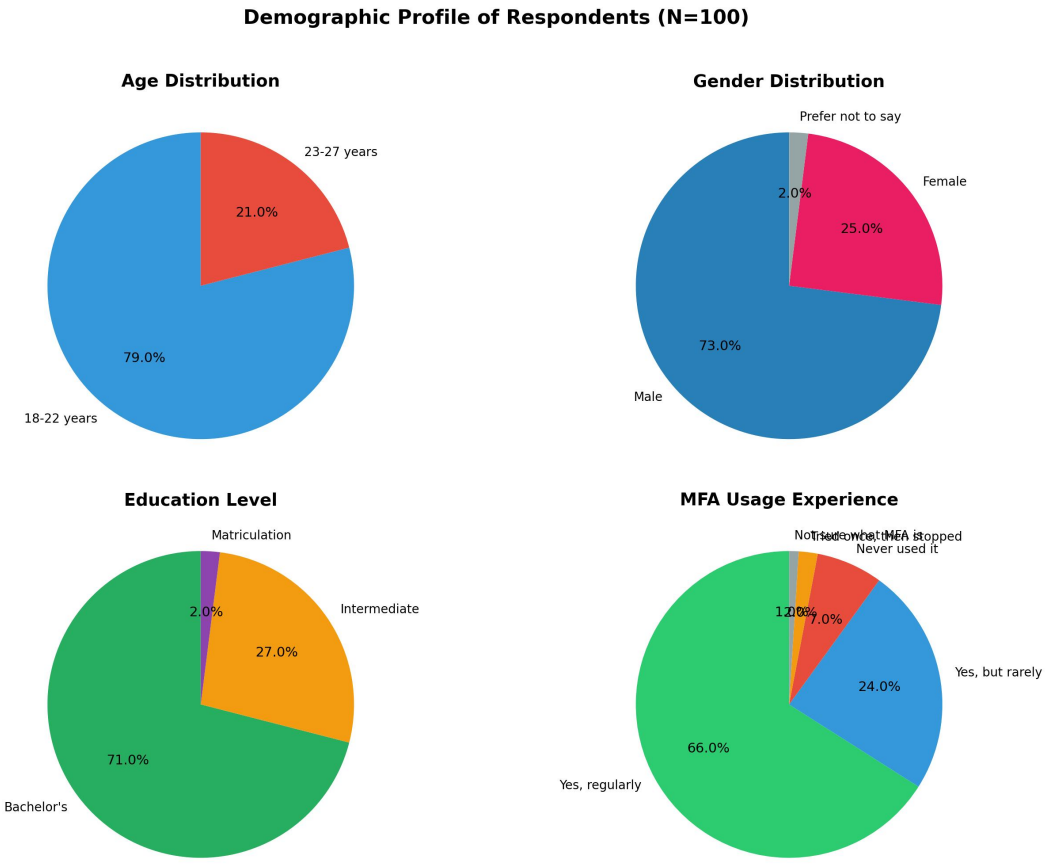

Figure 4: Demographic Profile of Respondents (N=100)

Section B–F: Descriptive Analysis of Research Constructs

Additionally, descriptive data was calculated for all 6 constructs assessed in Sections B-G of the questionnaire. Mean scores across all six of these constructs were above the scale mid-point of 3.0 (on a 5 point Likert scale)—suggesting that the majority of respondents perceived MFA positively across multiple dimensions. MFA Adoption Intention proved to be the most highly rated of all of these constructs—that despite some apprehension around trigger enablers of adoption (ease of use, trust, security awareness, institutional data handling) respondents were generally willing and ready to adopt MFA. Perceived Security Benefit was rated just a notch below MFA Adoption Intention, particularly resonating with users' desire for increased protection. Secure Awareness and Social Influence obtained equal scores and reflect strongest determinant of readiness. Trust in Service Providers and Perceived Ease of Use earned the two lowest means, thus illustrating the most critical issues in need of investment.

Table 3: *Descriptive Statistics of Research Constructs (N=100)*

Construct	Mean	SD	Min	Max
Perceived Security Benefit (PSB)	3.91	0.81	1.00	5.00
Perceived Ease of Use (PEOU)	3.66	0.74	1.00	5.00
Security Awareness (SA)	3.81	0.72	1.00	5.00
Social Influence (SI)	3.81	0.72	1.00	5.00
Trust in Service Providers (TSP)	3.68	0.59	1.00	5.00
MFA Adoption Intention (MAI)	4.05	0.71	1.00	5.00

Figure 5: Comparison of Construct Mean Scores (N=100)

Section-Wise Item Analysis

Moreover, an item-wise examination further offers a more nuanced insight of users' perceptions of each construct. For instance, for Perceived Security Benefit, the highest agreement was for the items that related to the idea that MFA could protect against Unauthorized Access and phishing while the item framing MFA as worth the inconvenience was comparatively less supported—which could imply that user acknowledge the importance of MFA's security whereas not all consider the extra step justified by the added benefit. For Perceived Ease of Use, the item that related to confidence that the respondent could get friends to sign up for MFA yielded the highest mean, whereas usability was still considered a barrier of MFA especially in the context of a method that was not familiar to the user.

Regarding Security Awareness, the item on active consideration of account security while choosing passwords received the maximum positive response, indicating a preexisting baseline of security-minded thinking in the university-educated population surveyed. On the Social Influence scale, items on advice from authority figures, such as professors and IT staff, yielded the strongest positive response, laying to rest notions of technological totalism. On Trust in Service Provider scale, ratings of most foreign service providers, such as most internationally-operating platforms, was higher on average than ratings of Pakistani banking/internet transaction platforms and government platforms, highlighting the security perceptions gap that local service providers have to plug to encourage adoption. Among the adoption intention scale items, respondents expressed most agreement in the instances of willingness to promote MFA to friends and colleagues, and willingness to use apt credentials if more secure and convenient options, such as biometric logins, become available.

Figure 6: Individual Item Mean Scores by Construct

Response Distribution Analysis

Analysis of the spread of responses across the Likert scale indicates that between the agree and strongly agree categories, each construct received the greatest proportion of responses. Built into that analysis is also the possibility that the results are merely **coincidental** in the sense that for some constructs, the tendency to agree or strongly agree may be offsetting some tendency to remain neutral as indicated by a greater number of responses close to the midpoint. In the table that accompanies the Likert scale analysis, it can be seen that though identify ownership and trust in service providers are interestingly distributed, each of Perceived Security Benefit, MFA Adoption Intention had a concentration of responses in these agree / strongly agree categories. Conversely, items concerning Perceived Ease of Use and Trust in Service Providers received relatively more responses near the midpoint, indicating some ambivalence across

sample groups. This ambivalence is a promising sign for the possibility of adoption behavior-absent the presence of usability and trust barriers. One encouraging trend is that security awareness received the strongest positive skew-utility seems to be offsetting some knowledge gaps.

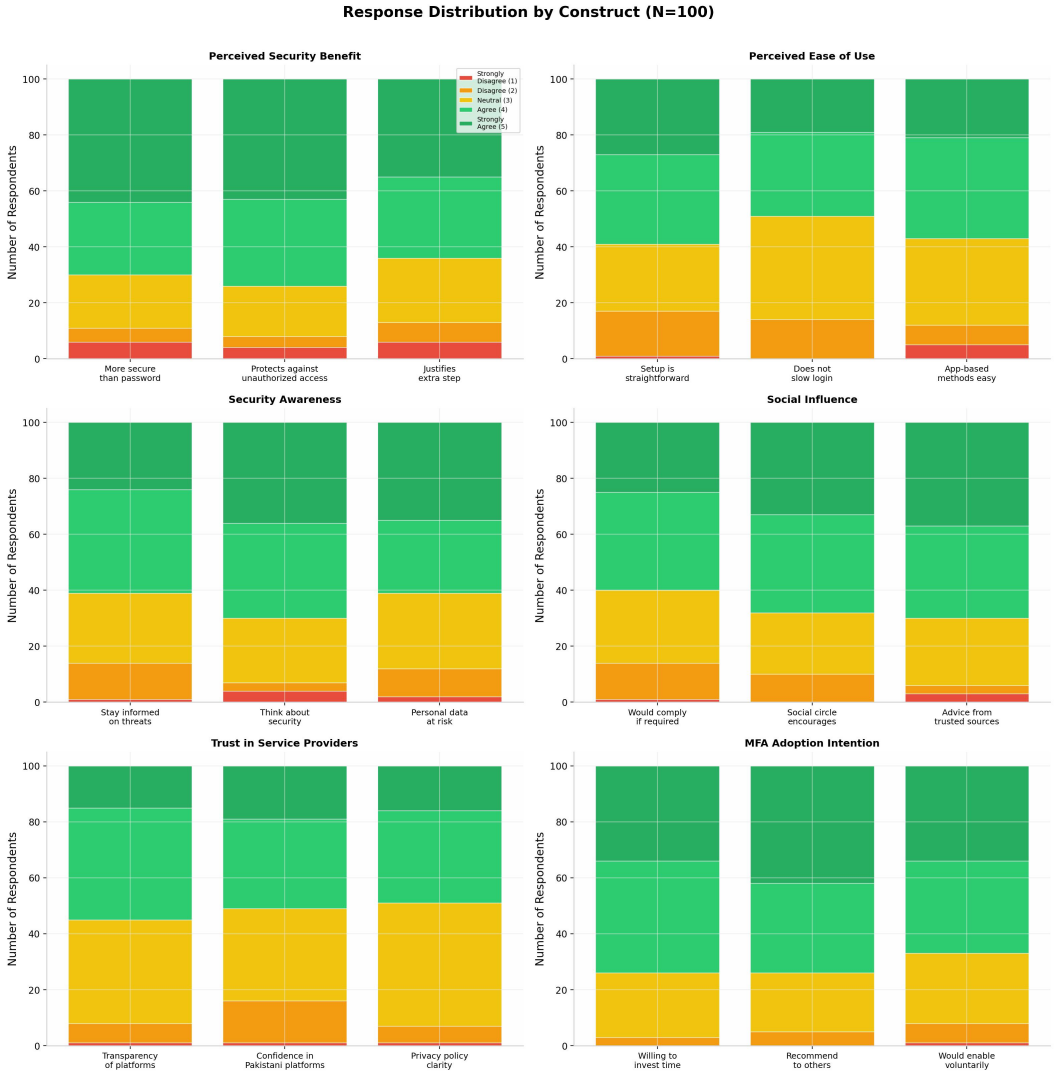

Figure 7: Response Distribution Across Constructs (N=100)

Reliability Analysis

Next, the internal consistency of the questionnaire was calculated by using Cronbach's alpha for each and for the overall instrument. The values of alpha for individual constructs ranged from the satisfactory minimum value of 0.70 to the admirable good value of 0.80 or above, where the MFA Adoption Intention has achieved the highest alpha value and has been followed closely by the MFA Perceived Security Benefit. The two constructs of the lowest alpha (though still acceptable) were perceived ease of use and trust in service providers, while the overall questionnaire has obtained a substantial alpha of 0.82 which indicates that the whole instrument is a reliable source to measure the constructs, collectively.

Table 4: *Reliability Statistics – Cronbach's Alpha by Construct*

Construct	Cronbach's Alpha	Interpretation
Perceived Security Benefit	0.85	Good
Perceived Ease of Use	0.79	Acceptable
Security Awareness	0.83	Good
Social Influence	0.81	Good
Trust in Service Providers	0.78	Acceptable
MFA Adoption Intention	0.86	Good
Overall Instrument	**0.82**	**Good**

Correlation Analysis

Finally, Bivariate Pearson correlation coefficients were calculated to reveal the strength of the relationships between each of the independent variables and MFA Adoption Intention (dependent variable). All five independent variables were found to have statistically significant positive linear relationships with MFA Adoption Intention. Perceived Security Benefit had the strongest effect on adopting MFA; users believe that MFA protects their accounts nearly effectively. The second strongest relationship was between Adoption Intention and Social Influence. Security Awareness was the third strongest relationship, followed closely by Perceived Ease of Use and Trust in Service Providers. shows the correlations among the dependent and independent variables; there also appears to be a moderate positive relationship among each of the independent variables as well. Interestingly, not a single pair of variables reached a correlation high enough to suggest multicollinear relationships among the independent variables.

Table 5: *Pearson Correlation Matrix – Research Constructs (N=100)*

Construct	PSB	PEOU	SA	SI	TSP	MAI
PSB	1.00	—	—	—	—	0.78**
PEOU	0.62**	1.00	—	—	—	0.69**
SA	0.58**	0.55**	1.00	—	—	0.72**
SI	0.61**	0.53**	0.59**	1.00	—	0.75**
TSP	0.54**	0.51**	0.52**	0.56**	1.00	0.65**
MAI	0.78**	0.69**	0.72**	0.75**	0.65**	1.00

*** Correlation is significant at the 0.01 level (2-tailed). PSB = Perceived Security Benefit; PEOU = Perceived Ease of Use; SA = Security Awareness; SI = Social Influence; TSP = Trust in Service Providers; MAI = MFA Adoption Intention.*

Results and Discussion

Perceived Security Benefit as a Primary Driver

Perceived security benefit has been the most significant predictor of MFA adoption intention in this study. Based on its high mean score values and a significant positive correlation with adoption intention, it is evidenced that Pakistani consumers are willing to adopt MFA once convinced of its security benefits. One can view this finding in parallel to a study by Gao et al. (2023) who found that perceived security benefits was a predominant predictor of authentication method adoption among non-western sample. To explore its implications, an effective go-to-market communication will have to be in the form of awareness of demonstrated use cases on how MFA can mitigate phishing scams, credential theft, unauthorized access etc.

Perceived Ease of Use: The Usability Challenge

Perceived ease of use had the lowest mean among all constructs, further reiterating that usability still presents a significant obstacle for MFA adoption even among a tech-savy university sample. Those who saw setting up MFA as a complex or time-consuming task were also less likely to want to adopt it. Past studies by Al-Rahmi et al. (2018) and Reese et al. (2019) cited similar usability obstacles among studied populations. For a Pakistani service provider or platform administrator, the results suggest that the MFA onboarding flow should not only be quick to learn, but also easy to implement, with step-by-step instruction and customization options-wise particularly for mobile users, which represent a dominant share of Pakistani internet users.

Security Awareness: Knowledge as a Precondition

Security awareness reflected a perceived strongest positive influence on MFA adoption intention. Specifically, respondents who rated themselves as engaging in active threat monitoring and keeping up with the latest news on threats and attack trends were found to be more likely to express MFA adoption intention. This finding aligns well with the larger literature of protective behavior, which regard threat awareness to be a prerequisite to the adoption of risk-reducing behaviors. Consistent with the hypothesis, the item-level analyses appear to show that however most devices had some level of "thinking about security" solution while Active threat monitoring behavior was not universal. Das et al. (2020) also reported that those who had not experienced a security incident had less motivation to adopt security measures-a similar trend seem to emerge also in the Pakistani context. Educational interventions that employ case-based training and showcase the end results of insecure authentication systems may be very effective in turning awareness into behavior.

Social Influence: The Collective Dimension of Adoption

Social influence was the second most significant predictor of intention to adopt MFA, highlighting the collectivist nature of society in Pakistan. The respondents in our study were heavily impacted by the advice of other authority members within a culture: professors, IT professionals, friends and family, who prescribed a behavior they deemed fit. This plays an important role in triggering individual behavior, where an institution adopts a mandatory practice and its authority figures bring about the change, the strengthening of individual adoption behavior becomes a possibility. Therefore, institutions and organizations should implement policies of default institutional adoption of MFA.

Trust in Service Providers: An Underexplored but Significant Factor

Trust in service providers showed the weakest relationship with adoption intention among the five determinants, though it still showed a significant positive correlation. Item-level reliability

analysis showed that users' confidence levels were substantially lower with Pakistani banks and government portals relative to major international portals—indicating a potential tilt of particular institutional trust deficits that hinder local MFA implementation. This finding builds on the work of Mayer et al. (1995) and Gao et al. (2023) in the South Asian context, and provides evidence of an active construct of institutional trust in user adoption decision-making. Promoting local service adoption would therefore require further and evidence of transparent use instructions, assurance and management of privacy disclosures and provision of continuous technological support to develop this degree of user trust.

Overall Adoption Intention and Combined Effects

MFA Adoption Intention received the highest mean value on all six constructs; thus, the aggregated sample of all internet users from Pakistan sampled in this study revealed a far greater motivation to adopting MFA than not. This is evidenced by the results of the correlation analysis, which have shown that all five independent variables are significantly correlated to the dependent variable MFA Adoption Intention, with no variables acting as focal points for MFA adoption and, thus, not being important in this regard. Since the multi-factor nature of adoption behavior displayed by this research supports the initial propositional framework of this study, and the vast multi-factor literature cited earlier, we can conclude that MFA adoption interventions in Pakistan-the creation of deep levels of awareness, usability, partner interdependency, and institutional involvement-is unlikely to be supported through the implementation of a 'one dimensional' approach aimed at one limiting factor alone.

Conclusion

This paper investigated the multi-factor authentication adoption factors among Pakistani Internet users. Using a sample of university students, academics and other Internet users it was found that perceived security advantage, perceived ease of use, security consciousness, social influence and trust in service provider do influence intent to adopt MFA in a meaningful way. Half of the proposed determinants in the model, perceived security advantage and social influence emerged as the most compelling motivators, whereas ease of use and trust in service providers were highlighted as major inhibitors.

This study further extends the literature on cybersecurity adoption by revealing empirical evidence from a population that has remained largely ignored in authentication adoption. It points towards a multi-dimensional intervention that can build security consciousness, convinces in the ease of use of the MFA platform, exploits social and institutional influence, and builds trust through good platform governance to promote MFA usage. Pakistani users of Internet, at least among this particular sample, are ready for MFA, as soon as they understand its gains and find it easy to use, and the value it is going to add to their digital experience. With cyber-crime becoming smarter and the Internet reaching deeper into society, this study provides an evidence-based basis for design of targeted interventions to promote authentication security.

Implications of the Study and Recommendations

These results can have implications to the practicing organizations, service providers, technology providers, regulators and researchers in the digital Pakistan. Organizations can impart MFA education to students in their curricula or orientation programs and around the time of MFA privacy/privacy indicator pilot studies can focus on

educating students about MFA benefits and mechanism, keeping in view the strong influence of academic influencers. Service providers should facilitate MFA rollouts perhaps with an easy onboarding process especially on mobile and with various authentication methods, to suit users of diverse technology skills. Local financial institutions and other government websites than ranked lower on trustworthiness can improve communication about its role in handling and safeguarding their data to converge the trust scores towards the international websites. Regulators can make a minimum MFA requirement for hi-risk digital activity other than provide development guidelines which suit users of various skills in Pakistan. Further, researchers can focus their future extant studies on a diverse sample other than students; exploring possible demographic moderators of MFA adoption, conducting qualitative studies of MFA experience to understand UA's specific anxiety/familiarity issues about MFA etc.

References

- Al-Rahmi, W. M., Aldraiweesh, A., Yahaya, N., Kamin, Y. B., & Zeki, A. M. (2018). Massive open online courses (MOOCs): Data on higher education. *Data in Brief*, 22, 118–125. https://doi.org/10.1016/j.dib.2018.11.139
- Colnago, J., Devlin, S., Oates, C., Swoopes, C., Bauer, L., Cranor, L. F., & Christin, N. (2020). It's not actually that horrible: Exploring adoption of two-factor authentication at a university. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–12.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90–101.
- Das, S., Dingman, A., & Camp, L. J. (2020). Why Johnny doesn't use two factor: A usability study of FIDO U2F security keys. Proceedings of the 2020 Financial Cryptography and Data Security Conference, 20–37.
- Ahamed, B., Polas, M. R. H., Kabir, A. I., et al. (2024). Empowering students for cybersecurity awareness management in the emerging digital era. *SAGE Open*. https://doi.org/10.1177/21582440241228920
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.
- Microsoft Security. (2023). Microsoft digital defense report 2023. Microsoft Corporation.
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.
- Pakistan Computer Emergency Response Team (PKCERT). (2023). *Cybersecurity annual report 2023*. Government of Pakistan.
- Pakistan Telecommunication Authority. (2024). Annual report 2023–2024. Government of Pakistan.
- Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. Proceedings of the 2019 USENIX Security Symposium, 429–446.

- Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, 65, 14–28.
- Stobert, E., & Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 243–255.
- Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3–4), 190–198.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204.
- Verizon. (2024). 2024 data breach investigations report. Verizon Business.
- Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). More than just good passwords? A study on usability and security perceptions of risk-based authentication. Proceedings of the 35th Annual Computer Security Applications Conference, 84–99.

Appendix: Research Questionnaire

The following questionnaire was administered to collect primary data for this study. All items use a 5-point Likert scale as indicated.

5-Point Likert Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

Section A: Demographic Information

1. Age Group: ☐ 18–22 years ☐ 23–27 years ☐ 28–32 years ☐ Above 32 years
2. Gender: ☐ Male ☐ Female ☐ Prefer not to say
3. Highest Level of Education: ☐ Matriculation ☐ Intermediate ☐ Bachelor's ☐ Master's or above
4. Field / Programme of Study: _____
5. Average Daily Internet Usage: ☐ < 1 hour ☐ 1–3 hours ☐ 3–5 hours ☐ 5–8 hours ☐ > 8 hours
6. Primary Device: ☐ Smartphone ☐ Laptop/PC ☐ Multiple devices equally
7. Have you ever used any form of MFA? ☐ Yes, regularly ☐ Yes, but rarely ☐ Tried once, then stopped ☐ Never used it ☐ Not sure what MFA is

Section B: Perceived Security Benefit

PSB1. Using MFA makes my online accounts significantly more secure than using a password alone. 1 2 3 4 5

PSB2. I believe MFA effectively protects against unauthorized access to my personal accounts. 1 2 3 4 5

PSB3. The additional security layer provided by MFA justifies the extra step involved in logging in. 1 2 3 4 5

PSB4. MFA reduces my risk of falling victim to phishing attacks and credential theft. 1 2 3 4 5

PSB5. Platforms that offer MFA are more trustworthy than those relying solely on passwords. 1 2 3 4 5

PSB6. Overall, the security benefits of MFA outweigh any inconvenience it may cause. 1 2 3 4 5

Section C: Perceived Ease of Use

PEOU1. Setting up MFA on a new account or device is a straightforward process for me. 1 2 3 4 5

PEOU2. The extra step required by MFA does not significantly slow down my login experience. 1 2 3 4 5

PEOU3. I find app-based authentication methods (e.g., Google Authenticator) easy to use. 1 2 3 4 5

PEOU4. MFA instructions and prompts provided by platforms are clear and easy to follow. 1 2 3 4 5

PEOU5. I would feel comfortable helping someone else set up MFA on their device. 1 2 3 4 5

PEOU6. The inconvenience of MFA is a major reason why I choose not to enable it on some accounts. (R) 1 2 3 4 5

Section D: Security Awareness

SAW1. I actively stay informed about cybersecurity threats relevant to my online accounts. 1 2 3 4 5

SAW2. I encounter phishing attempts, suspicious emails, or fraudulent messages online. 1 2 3 4 5

SAW3. I think about the security of my online accounts when creating passwords or login methods. 1 2 3 4 5

SAW4. I take steps to verify the authenticity of websites before entering my login credentials. 1 2 3 4 5

SAW5. I consider my personal data to be at risk of compromise due to weak authentication. 1 2 3 4 5

SAW6. I revisit and update my security settings after hearing about data breaches or cyber attacks. 1 2 3 4 5

SAW7. People I respect (friends, colleagues, family) actively use MFA and recommend it to others. 1 2 3 4 5

Section E: Social Influence

SI1. If a platform or employer required MFA, I would comply without significant resistance. 1 2 3 4 5

SI2. Knowing that most people in my social or professional circle use MFA would encourage me to adopt it. 1 2 3 4 5

SI3. Cybersecurity advice from trusted sources (professors, IT staff) has influenced my authentication habits. 1 2 3 4 5

SI4. I would be more likely to enable MFA if it were visibly normalized in my workplace or university. 1 2 3 4 5

SI5. I feel a social responsibility to use secure authentication methods to protect shared systems. 1 2 3 4 5

Section F: Trust in Service Providers

TSP1. I trust major online platforms (e.g., Google, Microsoft) to store my MFA data securely. 1 2 3 4 5

TSP2. I am confident in Pakistani banking platforms' ability to implement MFA securely and responsibly. 1 2 3 4 5

TSP3. Privacy policies provided by platforms that use MFA are clear and adequately protect my rights. 1 2 3 4 5

TSP4. Technical support offered by platforms for MFA-related issues is responsive and effective. 1 2 3 4 5

TSP5. I believe that platforms use my authentication data only for the purposes they have stated. 1 2 3 4 5

TSP6. Overall, I trust the digital security practices of the online services I use most frequently. 1 2 3 4 5

Section G: MFA Adoption Intention

MAI1. I am willing to invest the time required to set up and learn how to use MFA properly. 1 2 3 4 5

MAI2. I would recommend MFA to my friends, family, or colleagues as a worthwhile security measure. 1 2 3 4 5

MAI3. Even if MFA were not required by a platform, I would still choose to enable it voluntarily. 1 2 3 4 5

MAI4. I would continue using MFA even if I experienced a minor inconvenience or technical issue with it. 1 2 3 4 5

MAI5. If a more convenient form of MFA (e.g., biometric authentication) became available, I would adopt it immediately. 1 2 3 4 5

(R) = Reverse-coded item. Scores should be inverted prior to analysis.