Scientific Research Publishing

iBusiness, 2026, 18(1), 33-43
https://www.scirp.org/journal/ib
ISSN Online: 2150-4083
ISSN Print: 2150-4075

Impact of 2FA in Angola Bank Transactions

Francisco Mayele Silva Costa, Mateus Padoca Calado, Pedro Sebastião Teta

ACITE-Academia de Ciências Sociais e Tecnologias, Luanda, Angola
Email: s.academica@acite.ao

How to cite this paper: Costa, F. M. S., Calado, M. P., & Teta, P. S. (2026). Impact of 2FA in Angola Bank Transactions. *iBusiness, 18,* 33-43.
https://doi.org/10.4236/ib.2026.181003

Received: November 28, 2025
Accepted: March 15, 2026
Published: March 18, 2026

Abstract

With the advent of formalization of the Angolan economy, the use of electronic payment systems and internet banking, access to which in the traditional model is via a static credential, has become increasingly common, presenting a high degree of vulnerability nowadays, exposing confidential information, sensitive or protected from unauthorized persons. Electronic payment systems are heavily dependent on ICTs and other emerging technologies (fintech) in which customers or users must authenticate themselves to access banking products and services. Unauthorized access to sensitive authentication information can result in financial losses and compromise the image and good name of a given financial institution, in addition to a loss of confidence in the customer's use of the electronic payment system and internet banking. Given the high rates of fraud and scams motivated by weak authentication systems (static credentials), there was a need to implement the second authentication factor (2FA) which adds another layer of security for accessing or carrying out a banking transaction. For this reason, we will take a look at the impact of the implementation of 2FA in the Angolan Payment System, as well as technologies and solutions to mitigate this problem that greatly affects Angolan families and companies.

Keywords

Welwitschia Mirabillis Platform, Risk, Security and Validation in Banking Transactions

1. Introduction

Economic operators must offer their customers access to their infrastructure resources to provide banking products and services. Despite the different objectives and needs of employees, partners, suppliers and customers, they all require some level of access to corporate information. The number of connections and resources to manage makes user verification complex. Despite increasingly high levels of threats and attacks, most Internet banking applications still depend on weak

authentication systems to police user access, as the traditional system uses static passwords as the main means of authentication (username and password).

The most common economic scams in Angola are carried out by well-organized groups of criminals usually made up of bank employees, a computer specialist to carry out cyber-attacks, Ministry of Justice employees to authenticate or falsify documents and issue second copy of identity cards and telecommunications operators for issuing a duplicate SIM card (SIM Swap) (Deloitte, 2020). It is known that most banking operations are linked to mobile phone numbers which are managed through banking applications in which, to carry out a transaction, the user receives a verification code via SMS or email to authorize a specific banking operation. This authentication model is very vulnerable as it is enough for the criminal to have a duplicate of the card in their possession as well as the victim's confidential information, nothing prevents the financial scam from being carried out, causing unprecedented losses to the victim.

2. Theoretical Foundation

According to IBM's most recent 2024 Cost of a Data Breach report, Phishing and theft or compromised credentials are the two most common initial attack vectors. These vectors were responsible for 15% and 16% of breaches, respectively, with Phishing taking first place by a small margin over stolen credentials, which was the most common vector in the 2023 report. Network operators as well as cloud providers were identified as the initial attack vector at 11%, followed by business email compromise at 10%. In 2023, for the first time, the report examined both day-zero vulnerabilities (unknown) as well as known vulnerabilities, defined as unpatched vulnerabilities, as the source of data breaches and found that more than 5% of breaches studied originated from known vulnerabilities that have not yet been corrected. **Figure 1** shows the level of penetration of the main vulnerabilities as well as the costs associated with them, as can be seen in **Figure 1**.

Two-factor authentication is a feature available on economic operators' digital platforms when accessing online products and services that adds an additional layer of security to the process of logging into bank accounts or carrying out a certain transaction, requiring the user to provide two forms of authentication.

According to the regulator Bank National of Angola (BNA) 2023 cybersecurity report, credential theft, phishing and social engineering are the main attack vectors in Angola.

Activating two-factor authentication for online accounts is therefore essential for a substantial increase in security (Roger, 2020a). The use of One Time Password (OTP) sent via SMS as a second authentication factor is a recurring fact, however, its use should only be considered for some types of accounts. For accounts that contain sensitive data, the use of SMS as a second authentication factor should not be considered (Roger, 2020b).

From mobile network security deficiencies to the SIM swapping method, the use of tokens via SMS should be considered for accounts that contain sensitive

data such as personal or financial data (Roger, 2020a, 2020b). According to Professor Dr. Pedro Teta, more than looking at financial literacy, we must work to strengthen digital literacy to mitigate financial crimes via mobile networks.

Table 1 presents some comparative data regarding the vulnerabilities of different authentication models in compromising the confidential data of users of electronic payment systems.

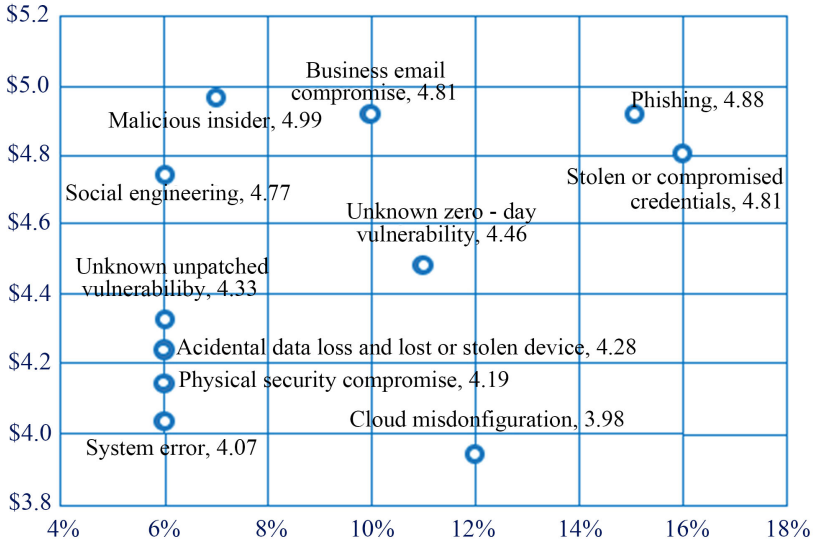

Figure 1. Measured in USD, percentage of all breaches (Cost of Data Breach Report, 2024).

Table 1. Comparative table of SMS and APP Authentication.

Types of Authentications	Advantages	Disadvantages
SMS	They are not encrypted in transmission. Easier recovery if your mobile device is lost or stolen. Easy implementation and low integration cost.	Requires connection to the mobile network. It presents a high degree of vulnerability. SIM Swap and SS7 attacks are common.
APP Authentication	Does not require connection to a mobile network or internet. The same application can generate tokens for multiples accounts.	Susceptible to loss or theft of the mobile device. Critical for generating backup codes.

3. Welwitschia Mirabillis Platform

To analyze the impact of 2FA, we will present a platform developed using the Zero Trust Security Model that implements 2FA with authenticator software.

If we can generate the E2E (server and mobile application) dynamic password without it being transmitted over the network, it will be the icing on the cake in terms of security (Krawczyk et al., 1997). This desire is possible through authenticator software. This security method is so effective that economic operators, companies and organizations around the world use it to monitor and protect their information, assets and networks. In addition, we recommend that end users adopt this authentication method to protect their own accounts and available data (Costa, 2024).

3.1. Views of W. Mirabillis Platform

In this session, the operating principle of the W. Mirabillis Platform is described, as well as the layout of the web application, whose authentication method is carried out using the one-time password-based cryptographic algorithm (TOTP) and authenticator software.

3.1.1. Low Fidelity Prototype Home Page

The main objective is to present the different layouts for accessing the products and services available on that platform. In the top right corner, a *dropdown1* button is available with the following links: My account, login, create account and recover password.

3.1.2. Low Fidelity Prototype Login Page

The W. Mirabillis application login page allows users to log in by entering their static credentials (email and password) that correspond to the first level authentication. Once this access information has been validated, the user will be redirected to the authentication screen that corresponds to the second level of authentication, as we can see in Figure 2:

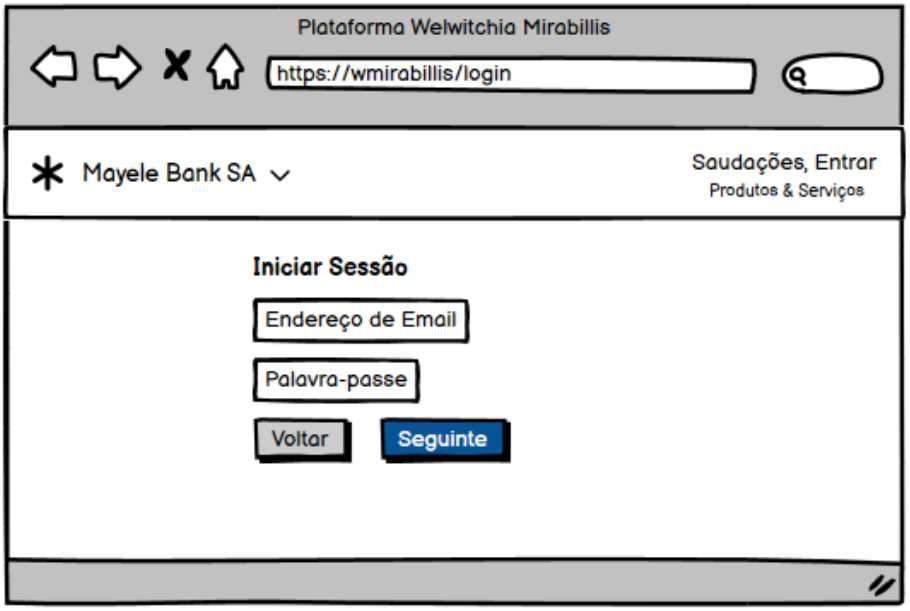

Figure 2. Low fidelity prototype login page.

3.1.3. Low Fidelity Prototype Authentication Page

In the second level of authentication, the user must enter the validation code generated by the authentication App, in this specific case by Google Authenticator. W. Mirabillis Platform uses 6 digits token with 30 seconds lifetime, i.e., the authentication App generates the codes in every 30 seconds, this being the time interval that user must authenticate yourself in the system. If the user exceeds this period, the token expires and you will need a new code available in the application (Figure 3).

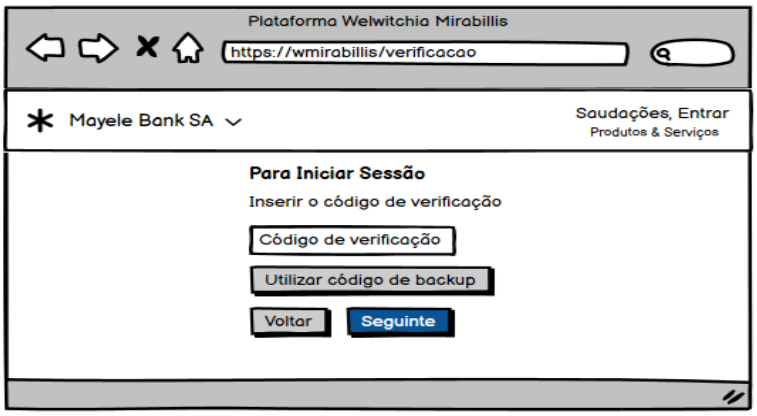

Figure 3. Low fidelity prototype verification page.

This functionality increases the cyber security resilience of W. Mirabillis Platform against malicious people or hackers, preventing the consummation of personification crime. Cyber-attacks expose user account login information, but are unlikely to expose 2FA generated by any authenticator application. Figure 4 shows the account dashboard of a user who successfully completed both stages of authentication process.

Figure 4. Low fidelity prototype operations screen.

3.2. W. Mirabillis Platform Security

With the use of 2FA by authentication APP, hackers or criminals begin to depend on the victim's account holder to carry out fraud or crime, in this sense and with the level of financial literacy as well as cybercrimes, in general, the volume of attacks has been falling significantly.

4. Methodology

In this chapter, the results of the research carried out to assess the financial literacy of users of electronic payment systems in Angola and assess the level of use of 2FA

will be presented.

4.1. Research Methodology

Research was carried out to study the relationship between privacy concerns, security, perceived risk and how these elements would relate to the level of customer trust in electronic payment systems associated with the implementation of 2FA. In a sample of approximately 111 participants, they were randomly invited to respond to the survey. The target audience included employees and students at ACITE, teachers and students at the Industrial Polytechnic Institute of Zango 8000, teachers and students at the Faculty of Engineering at UAN, small and medium-sized entrepreneurs who use e-commerce as support to boost their businesses. Table 2 presents an estimate regarding the demographics of the participants.

Table 2. Demographics of survey participants.

Survey Result			
Total number of participants	**111 participants**		
Gender	Male: **79.3%**	Female: **20.7%**	
Real-time account banking transaction notifications	Yes: **38.5%**	No: **33.7%**	Not always: **27.9%**
Electronic Payment System Security	Yes: **58.3%**	No: **41.4%**	
Victims of scam or financial fraud	Yes: **25.9%**	No: **65.7%**	Perhaps: **8.3%**
Importance of 2FA in critical accounts	Yes: **34.2%**	No: **65.8%**	

4.2. Data Analysis

In order to determine the safest method for the user to receive the verification code to access or validate a banking transaction, when carrying out the survey, we found that 28.6% of participants were unaware of the pros and cons of the different methods. of authentication for this reason, they only use SMS, it was also found that the users' voting intention changed as they became clearer about the risks associated with this sending method (SMS).

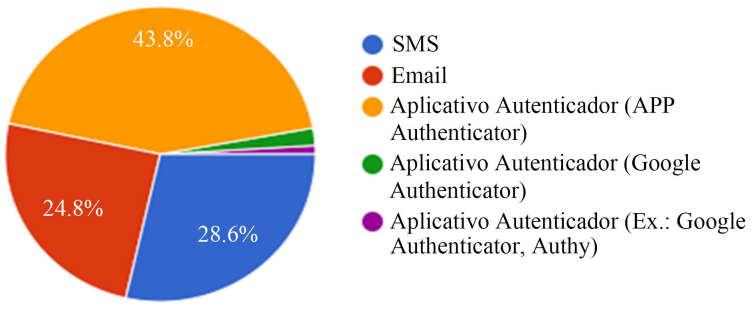

Figure 5. Survey result regarding 2FA shipping method [(Costa, 2024). Security in Banking Transactions].

It was also found that the most enlightened users are in most cases those with

critical account, who advocate the use of safer mechanisms such as authenticator application to guarantee better security for their assets or credential data. These correspond to 46.7%, while the use of sending by e-mail accounted for 24.8% of voting intensions. It was possible to verify that most of the participants who think that E-mail or SMS are safe have as reference the complexity of using an APP or the cost associated with its use, using simpler system, putting security at risk (**Figure 5**).

In order to assess how users of electronic payment systems think about solving the problem of personification as well as non-repudiation, out of a total of 105 survey participants, only 43.8% felt confident in using the knowledge test, while 56.2% guarantee that the use of 2FA, that is, the combination of poof of knowledge + possession, provides greater security in accessing and validating banking transactions, as can be seen in **Figure 6**.

Security solutions as well as the analysis of the main attack vectors were treated as mentioned by Calado, M. Padoca, which recommends paying special attention to services available via the web and adopting measures to prevent attacks (Calado et al., 2019).

Calado (2015: p. 129) reinforces the need for a 3-layer architecture to ensure security and good response to user requests. The solution presented in this work adopts the MTV architecture to ensure code modularization, scalability and ease of maintenance (Ramos et al., 2020).

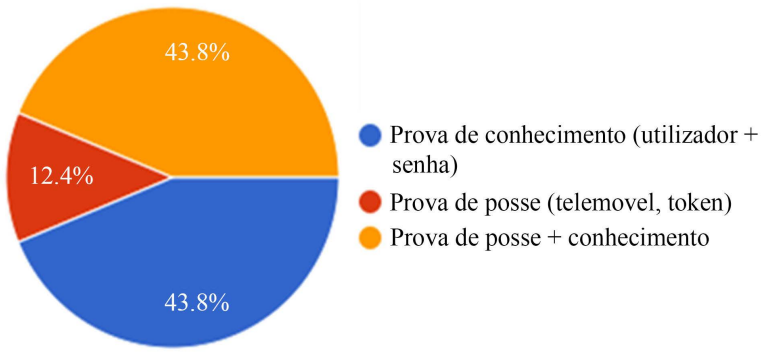

Figure 6. Result of the survey regarding unauthorized access (Costa, 2024).

5. Impact of 2FA in Angola Economy

Nowadays, critical financial infrastructures must rely on 2FA as a defense mechanism against cyber threats.

The Welwitschia Mirabillis platform supports the implementation of RFC4226 and RFC6238 to reinforce security when accessing banking products and services. (Costa, 2024).

Below is a comparative table that represents the financial impact by technology with the implementation of MFA (**Table 3**).

The application of security mechanisms that aim to reinforce the user authentication system for accessing and carrying out banking transactions based on the TOTP APP protocol (anti-fraud control systems) generates a significant Return

on Investment (ROI), not only by reducing direct losses, but also by indirect benefits such as compliance with the regulator's standards and protocols, reputation and operational efficiency.

Table 3. Comparative table of financial impact by technology.

Method	Cust/User/year	Fraud Reduction	Angolan Reality
SMS OTP	$0.85	55% - 65%	Limited (coverage)
App Authy	$1.820	70% - 80%	Ideal for urban areas
Facial Biometrics	$2.50	85%+	Excellent (but expensive)
Token HSM	$4.00	90%+	Ideal for corporate environment

5.1. Treats and Containment Measures

The first "phishing" emails targeting online financial systems were seen in 2001, as a "911 Identity Verification Post" following the September 11 attacks on the World Trade Center. From 2004 onwards, the industry has seen a dramatic increase in attacks against large and small financial institutions around the world.

Despite the diversity in attack methods, most aim to achieve the same objective: obtaining confidential user information, such as usernames, passwords and credit card numbers, access credentials and that is where the problem lies. Once obtained, they can be used by the attacker to impersonate the customer to commit financial fraud.

5.2. Second Authentication Factor (2FA)

Although it is useful to try to combat specific attacks motivated by the vulnerability of the current authentication system with a strong dependence on static credentials for access and validation of a banking transaction, what is recommended nowadays is the addition of another layer of security to the current model that presents itself as the only long-term strategic solution with the implementation of MFA (2FA) technology through the OTP cryptographic protocol. Any One-Time Password algorithm is only as secure as the application and the authentication protocols that implement it (RFC 4226).

In general, economic operators create accounts for individuals and companies to offer their customers the convenience of accessing banking products and services via the internet, as well as through a wide range of banking applications or *e-banking*2. To access your economic operator's portal, customers or users must authenticate if they have an account created or after the registration process. Because of possible clock drifts between a client and a validation server, we RECOMMEND that the validator be set with a specific limit to the number of time steps a prover can be "out of synch" before being rejected (RFC 6238).

5.3. Attacks against 2FA

A small number of successful attacks against 2FA-enabled internet banking sys-

tems have led to press reports that 2FA as a general approach has been "broken." The reality is a little more complex, as we will discuss below.

An attacker can obtain a valid OTP from a user using the same methods used to obtain a static password. If the bank has implemented a simple system with 2FA used only for login, this attack could be successful. The level of financial literacy of users of electronic payment systems plays an important role here.

To mitigate or eliminate this risk, it is necessary to understand how attackers operate. It is known that attacks are carried out by well-organized groups, each with a specific function competing for the same objective. The attack fronts cooperate with each other, each providing a specific service: creating a fake website, sending spam by email, stealing access credentials and, finally, with the credentials incalculable losses will be applied to the victims' bank account.

5.4. Fraud and Risk Reduction

Failing to invest in the implementation of 2FA in electronic payment systems can be seen as a 'time bomb', waiting for an explosion of fraud. The insecurity intrinsic to the traditional authentication model (without 2FA) drives attackers' rapid ability to access victims' confidential data through advanced attacks.

As we know, the critical infrastructures of national banking are under constant attack, the fraud detection and prevention mechanisms (IDS/IPS) are good, but not perfect; associated with the fact that the latter cannot be everywhere at all times. Most banks currently accumulate high losses inherent in full refunds to customers who are victims of fraud, leaving the bank exposed to primary fraud. Although this scenario can be resolved through rigorous internal and external audit processes, these are expensive and time-consuming. Sharing the risks by forcing active customer participation in each transaction, the implementation of 2FA reduces primary fraud for customers associated with the crime of impersonation and increases the scope for the bank to exempt itself from liability in suspicious cases.

Unlike many banks in Angola, where customers use static credentials to access their bank accounts online, the W. Mirabillis platform has added an additional layer of security, allowing users to choose the SMS or TOTP APP authentication method in the settings, as is the case in several countries, which increases cyber resilience against cybercrime. In this work, it is recommended to choose an authenticator APP with backup capacity with access to different electronic devices, to guarantee access in case of theft or loss.

The research was carried out on a restricted group of users of electronic payment systems which in Angola are for people over 18 years of age. The Angolan government, aware of the challenges of strengthening security in critical infrastructure such as the financial sector, launched the Iluminar Angola project to increase mobile network coverage in all municipalities and strengthen digital and financial literacy. For the financial sector and beyond, one of the tools that helps mitigate fraud is rigorous internal and external audit processes, reinforcing the

concepts of implicit trust and zero trust, which are discussed in depth in this work. Almeida argues that one of the studies that best explains the factors in the occurrence of fraud is based on the Fraud Triangle theory developed by Donald Cressey, which presents an important insight into the motivation for committing fraud (Almeida, 2010).

Acknowledgements

I would like to thank my beloved wife Welwitschia da Costa, my children Kitoânia da Costa, Mayele da Costa, Alan da Costa, Alana da Costa, Weza da Costa and Vladmir da Costa for their support during this challenge. They understood and accepted being without the presence of their husband and father during the period of classes and seminars, as well as on the weekends and holidays dedicated to the completion of this work.

Special thanks to Professor Mateus Padoca Calado, who was in fact supervisor of this master's project and who was unable to be a member of the jury due to the interpretation imposed by the legal diploma that governed the submission of the dissertation to the Angolan Academy of Social Sciences and Technology. A sincere thank you for your support, vote of confidence, patience and understanding. Your critical and truthful approach and the suggestions you gave were invaluable for the completion of this work. The freedom you gave me to explore my own paths and points of view was precious and, I believe, rare.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Almeida, M. C. (2010). *Audit: A Modern and Complete Curse* (7th ed.). Atlas.

Calado, M. P. (2015). *Angolan Emergency Medical Service: Optimization Using Multi-Agent Systems*. Luanda-Angola.

Calado, M. P., Ramos, A. A., & Jonas, P. (2019). An Application to Generate, Correct and Grade Multiple-Choice Tests. In *2019 6th International Conference on Systems and Informatics (ICSAI)* (pp. 1548-1552). IEEE. https://doi.org/10.1109/icsai48974.2019.9010132

Cost of Data Breach Report (2024). *IBM Security Report 2024*. USA: New Orchard Road Armonk, NY 10504. IBM Corporation & Ponemon Institute.

Costa, F. M. S. (2024). *Security in Banking Transactions: 2FA Implementation Proposal Using TOTP Protocol and Software Authenticator*. Luan-da-Angola.

D'Raihi, Pei, M., Symantec, Rydell, J., & Partwise (2011). *TOTP: Time-Based One-Time Password Algorithm*. Inc. RFC6238.

Deloitte (2020). *Fraud Survey Angola*. Deloitte & Touche.

Krawczyk, H., Bellare, M., & R. Canetti (1997). *[RFC2104] "HMAC: Keyed—Hashing for Message Authentication"*.

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *HOTP: An HMAC-Based One-Time Password Algorithm*. RFC4226.

Piqueras Roger, J. (2020a). Security Analysis of SMS. *International Journal for Digital Society, 10,* 1556-1561.

Piqueras Roger, J. (2020b). Security Analysis of SMS as a Second Factor of Authentication. *Communications of the ACM, 63,* 46-52. https://doi.org/10.1145/3424260

Ramos, A., Calado, M., & Antunes, L. (2020). A Gift-Exchange Model for the Maintenance of Group Cohesion in a Telecommunications Scenario. In F. Herrera, K. Matsui, & S. Rodríguez-González (Eds.), *Distributed Computing and Artificial Intelligence, 16th International Conference* (pp. 189-196). Springer International Publishing. https://doi.org/10.1007/978-3-030-23887-2_22