



# Security Guidelines for the Design of ATM Interfaces

Fiorella Falconi<sup>(✉)</sup>, Claudia Zapata<sup>(✉)</sup>, Arturo Moquillaza<sup>(✉)</sup>,  
and Freddy Paz<sup>(✉)</sup>

Pontificia Universidad Católica del Perú, Lima 32, Lima, Peru  
{ffalconi, zapata.cmp}@pucp.edu.pe,  
{amoquillaza, fpaz}@pucp.pe

**Abstract.** In Peru, 41% of the population over 18 is banked and 76% of them use an Automatic Teller Machine or ATM. However, in some cases the interaction between the users and the ATM (and the User Experience in general) could be frustrating and presents inconveniences in topics about trust and security, considering that clients are mainly carrying out operations that involve withdrawal and depositing of their own money in cash. In that sense, the influence of security (and the perception of security by the user) in the experience of using ATM, given their nature and form of use, has been evidenced. According to the above, we found in the literature that specific design and heuristic guidelines have been proposed for the usability of ATM interfaces, but no specific guidelines for other relevant aspect such as the security of those interfaces. The main objective of this work is to provide a proposal of security guidelines for the design of ATM interfaces, which complement existing guidelines on other facets of the User Experience, such as, Usability and Accessibility, which seeks to strengthen the User Experience of the product. To obtain the mentioned guidelines, a compilation of good practices, recommendations and guidelines found in Peruvian and international literature and regulations was made. For the validation of this proposal, these guidelines were validated through expert judgment by three ATM interface design experts and four domain experts working in 3 of the most important banks in Peru. As a result, we proposed seven ATM interface security guidelines and their respective definitions. From this work, we can conclude the importance of not just evaluating Usability but also complementing security issues when it comes to a channel as sensitive as ATMs, and in that sense, for this domain, consider security as an important part of the User Experience.

**Keywords:** Security guidelines · Automated Teller Machine · Design interfaces · ATM interfaces

## 1 Introduction

Transactions in ATM channel have become a basic and recurring activity in people. In Peru, 41% of people over the age of 18 are clients of a bank or financial institution, and the most used channel among them is still the ATM. A study from IPSOS Peru indicates that 76% use ATM to carry out a transaction, positioning this channel over

branches, banking, agents and other digital channels [1]. This high demand of the channel is reflected in the number of ATM that the country has an approximate of 107 ATM per 100 thousand adult inhabitants [2]. This establishes to Peru as the second country with greater access to ATMs in the region.

However, in some cases, the interaction between users and ATMs could be frustrating and inconvenient. If we consider that a good interface design is necessary to raise Usability levels, it is evident that with regard to ATM, there is still much to do to improve the design of its interfaces [3].

Although there is little information on how to design interfaces for ATM, especially if we compare it with the amount of principles and guidelines that have been proposed for web interfaces [4], they have begun to propose guidelines, principles and heuristics focused on ATMs [5], and also formal methods for designing specific interfaces for ATMs [6].

The ATM machine, given its operations with cash and sensitive customer information, safety issues must be a priority. Nevertheless, it is not easy to bring these security elements to users, so it is necessary to incorporate an adequate process to design for reaching a good User Experience (UX). UX is understood as “the feeling, emotional response, assessment and satisfaction of the user regarding a product, the result of the phenomenon of interaction with the product and interaction with its supplier” [7]. It is considered of great importance to incorporate security aspects from the beginning of the interface design, considering the balance between User Experience points and security [8].

In this sense, in the context of an adequate UX, Usability and Security are closely related, and although they are sometimes considered as opposed, they are an important part of the overall experience. In that sense, the balance should be sought and both factors considered for better interfaces [9].

## **2 Relevant Concepts**

### **2.1 Automatic Teller Machine**

Automatic Teller Machine (ATM) is a computerized telecommunications device that provides, in real time, access to the clients of a financial institution to their bank accounts in a public space without intervention of the administration of the financial institution [10]. The customer commonly is identified by inserting the card and entering a personal identification number (PIN). This process allows customers to service themselves and to perform the operations available according to their bank.

### **2.2 User Experience**

According to ISO 9241, user experience is a person’s perceptions and responses that result from the use or anticipated use of a product, system or service. Three aspects that influence the User Experience are the following: the system, the user and the context of use [11].

## 2.3 Security

Security is interpreted as the perception of security that customers have when making a transaction from the beginning to the end of it. The lack of security perception causes the client not to use a certain channel to carry out their transactions. For this reason, perceived security is the extent to which a customer believes that a channel is safe to perform their bank transaction [12].

## 2.4 User Interfaces

A User interface is the component of a system with which the users interact, receive information and control to perform tasks in the system [12]. An example of an ATM user interface is shown in Fig. 1.



Fig. 1. Main screen ATM HSBC-México (HSBC, 2019)

## 3 Literature Review

In the literature, we did not find a consolidated and validated list of guidelines for ATM security, but some recommended practices were found that increase the perception of customer security when interact with ATM. The search was carried out in the databases: Scopus, IEEEXplore, ACM Library Digital and SpringerLink, with a PICOC chain and between 2010–2019, we obtained 9 relevant articles as a result. The guidelines collected are based on the need to convey to users confidence and clarity when interacting with ATMs [13].

In addition, we considered the security requirements of the PCI DSS [14], handbook TCR [15] and resolutions of the Superintendence of Banking and Insurance of Peru [16, 17] have been reviewed. PCI DSS is the global data security standard, adopted by card brands for all entities that process, store or transmit cardholder data

and/or confidential authentication data. Table 1 shows the security guidelines collected in a first proposal.

**Table 1.** ATM security guidelines collected

Guidelines	Definition	Obtained from
1. Mask sensitive data	Avoid showing sensitive keys and data (card number, hpv, phones, mail, etc.) to avoid shoulder-surfing	[14, 18]
2. Provide relevant information	The client must have the possibility to consult information that he considers relevant. Especially in cases where you hire a product at the ATM (Costs, commissions, etc.)	[15–17]
3. Logout for time-out	After a certain time without customer interaction with the ATM, the session must be concluded	[19]
4. Login information	Give login information and information that the client recognizes as their private session. E.g.: Recent transactions	[13]
5. Session management	Give information on how to log in and how to end the session	[13]
6. Notifications and alerts	Send notifications and alerts of irregular activity in ATM	[13]

## 4 Validation

To validate the security guidelines compiled for ATM, an interview was conducted with seven experts, four domain experts from the three main national banks and three experts on ATM interface design. We asked for their expert opinion on each guideline and was requested a score from 1 to 5 according to the importance considered for each guideline. Table 2 shows the score of each expert about each guideline.

**Table 2.** Expert evaluation about guidelines

Guideline	Score for each expert							Average score
	N°1	N°2	N°3	N°4	N°5	N°6	N°7	
1. Mask sensitive data	3	3	4	5	5	5	5	4.29
2. Provide relevant information	5	5	4	4	4	1	4	3.86
3. Logout for time-out	4	1	3	2	4	5	4	3.29
4. Login information	4	3	2	5	5	5	3	3.86
5. Session management	5	5	4	1	4	4	4	3.86
6. Notifications and alerts	4	4	5	4	5	5	4	3.86

According to the results of the interviews and the scores, we decided to make some modifications by integrating the information collected, with the aim of grouping similar topics, clarifying the scope of each guideline and giving a more complete definition. The updated list of guidelines is shown in the Table 3.

**Table 3.** Security guidelines

Guideline	Definition
1. Protection of sensitive data	Use mechanisms to prevent other people from seeing information such as passwords, phones, balances, etc. It could be at the request of the client
2. Show information clearly	The relevant information must be clearly displayed so that the user can identify the points of interest
3. Log for time-out	After a certain time without customer interaction with the ATM, the session must be concluded. Important that the client knows how much time he has available
4. Visible security	Make evident in the interfaces the protection measures available to the cashier
5. Build trust	Always show the client how to manage your session
6. Notifications and alerts	Send notifications and alerts of irregular activity in ATM
7. Security depending on the risk	The amount of validations must depend on the risk to which the client is exposed, this may include validations at night, for amounts, etc

## 5 Conclusions and Future Work

This work showed that there are points related to the perception of security that contribute significantly to the User Experience on the ATM domain. One of the most important points was the one that covers the subject of sensitive customer information that is displayed on the screen, for reasons of shoulder-surfing and insecurity.

We consider that these seven proposed guidelines cover important aspects for the client when interacting with an ATM. These guidelines will be more or less important depending on a set of factors: the area where the ATM is located, current date and time, customer profile, if the ATM is inside or outside a branch, among others. However, since the ATM channel is characterized by having different types of customers, locations, and features, of, we recommend considering the present proposal in any processes of design, redesign or evaluation of ATM interfaces.

Finally, we consider as future work, the validation of this proposal in real cases in the industrial context, specifically in ATM design and redesign projects.

## References

1. IPSOS. Bancarización del peruano (2018). <https://www.ipsos.com/es-pe/bancarizacion-del-peruano>
2. Redacción Economía. Inclusión financiera: ¿Cómo avanza el Perú frente a otros países de la región? El comercio (2019). <https://elcomercio.pe/economia/peru/inclusion-financiera-avanza-peru-frente-otros-paises-region-noticia-635376>
3. Curran, K., King, D.: Investigating the human computer interaction problems with automated teller machine navigation menus. *Interact. Technol. Smart Educ.* **5**(1), 59–79 (2008). <https://doi.org/10.1108/17415650810871583>
4. Moquillaza, A., Molina, E., Noguera, E., Enríquez, L., Muñoz, A., Paz, F., Collazos, C.: Developing an ATM interface using user-centered design techniques. *Lecture Notes in Computer Science*, pp. 690–701 (2017). [https://doi.org/10.1007/978-3-319-58640-3\\_49](https://doi.org/10.1007/978-3-319-58640-3_49)
5. Chanco, C., Moquillaza, A., Paz, F.: Development and validation of usability heuristics for evaluation of interfaces in ATMs. In: *Design, User Experience, and Usability. Practice and Case Studies*, pp. 3–18 (2019). [https://doi.org/10.1007/978-3-030-23535-2\\_1](https://doi.org/10.1007/978-3-030-23535-2_1)
6. Aguirre, J., Moquillaza, A., Paz, F.: Methodologies for the design of ATM interfaces: a systematic review. In: *Human Systems Engineering and Design*, pp. 256–262 (2018). [https://doi.org/10.1007/978-3-030-02053-8\\_39](https://doi.org/10.1007/978-3-030-02053-8_39)
7. Hassan, Y.: *Experiencia de Usuario: Principios y Métodos* (2015). [http://yusef.es/Experiencia\\_de\\_Usuario.pdf](http://yusef.es/Experiencia_de_Usuario.pdf)
8. Galvy, C.: La experiencia de usuario en la seguridad de la información de la banca en línea. <https://revista.seguridad.unam.mx/print/2625>. Accessed 29 Jan 2020
9. Kaında, R., Fléchais, I., Roscoe, A.: Security and usability: analysis and evaluation. In: *2010 International Conference on Availability, Reliability and Security* (2010). <https://doi.org/10.1109/ares.2010.77>
10. Khalifa, S.S.M., Saadan, K.: The formal design model of an automatic teller machine (ATM). *Lect. Notes Inf. Theory* **1**(1), 56–59 (2013). <https://doi.org/10.12720/lnit.1.1.56-59>
11. ISO. ISO 9241-210:2010, (122457) (2010)
12. Chang, H.H., Chen, S.W.: Consumer perception of interface quality, security, and loyalty in electronic commerce. *Inf. Manag.* **46**(7), 411–417 (2009). <https://doi.org/10.1016/j.im.2009.08.002>
13. Subsorn, P., Limwiriyakul, S.: A comparative analysis of internet banking security in Thailand: a customer perspective. *Procedia Eng.* **32**, 260–272 (2012). <https://doi.org/10.1016/j.proeng.2012.01.1266>
14. PCI. PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard (version 3.2.1) (2018). [https://www.pcisecuritystandards.org/documents/PCI\\_DSS-QRG-v3\\_2\\_1.pdf?agreement=true&time=1534870826847](https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1534870826847)
15. BBVA. TCR, los principios que están cambiando la forma de trabajar de BBVA (2017). <https://www.bbva.com/es/tcr-principios-estan-cambiando-forma-trabajar-bbva/>
16. SBS. Resolución SBS N°2011 (Artículo 10) (2011). <https://intranet2.sbs.gob.pe/preproyectosApp/download.asp?f=1625LC45QRDTKOEEKW6IDK4Y0XYASNOAN.PDF>
17. SBS. Resolución SBS N°8181-2012 (Artículo 13) (2012). [https://intranet2.sbs.gob.pe/dv\\_int\\_cn/763/v4.0/Adjuntos/8181-2012.R.pdf](https://intranet2.sbs.gob.pe/dv_int_cn/763/v4.0/Adjuntos/8181-2012.R.pdf)

18. Adithya, P., Aishwarya, S., Megalai, S., Priyadharshini, S., Kurinjimalar, R.: Security enhancement in automated teller machine. In: 2017 International Conference on Intelligent Computing and Control (I2C2) (2017). <https://doi.org/10.1109/i2c2.2017.8321773>
19. Zhang, M., Wang, F., Deng, H., Yin, J.: A survey on human-computer interaction technology for financial terminals. In: 2012 Fifth International Conference on Intelligent Networks and Intelligent Systems (2012). <https://doi.org/10.1109/icinis.2012.65>