Multidisciplinary International Journal of Research and Development

Volume: 04 / Issue: 03 / 2025 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

Security and Vulnerability: Using One-Time Pin to Access Data for Online Transactions

Yshana Francine B. Alcantara[1], Christiffany B. Casas[2], Romalyn D. Dela Torre[3], and Gabriela C. Flores[4]

[1,2,3,4]College of Arts and Sciences, Departments of Statistics, Rizal Technological University, Boni Campus, Mandaluyong City, Philippines

Abstract— An increasing number of industries have been transformed with the aid of technology and technological advancements. Online transactions became more common in the digital age provided by banks as primary services today. As a result, online transaction systems enabled instant verification through one-time pins. The study explored the security and vulnerabilities of one-time pins in online transactions and focused on determining its effectiveness in preventing fraud. The study allowed researchers to better understand one-time pin vulnerabilities; provided important insights into improving digital systems and prioritizing security measures such as one-time pins for online transactions.

The researchers surveyed 180 working individuals in Mandaluyong City about their perceptions and experiences with one-time pins. Purposive sampling technique was employed in identifying individuals who matched the study's target respondents. Moreover, the researchers used the weighted mean, Mann-Whitney U-test, Kruskal-Wallis H-test, and percentage to ensure accurate data and generalize the findings.

The findings showed that many regular users of this authentication method perform online transactions, though majority of these individuals had an average level of technological knowledge. This study also identified common security problems and vulnerabilities associated with one-time pins across different profiles and found that demographic differences did not always influence users' perceptions of one-time pin security.

Keywords— One-Time Pin, Online Transactions, Security, Vulnerability.

I. INTRODUCTION

In today's world, many changes are brought about by innovation and technology. Modern technology has enabled many ideas to become realities. In recent years, many industries have been transformed by technology, particularly the financial industry, which is constantly evolving. According to Sutton (2023), technology is revolutionizing every important part of finance because finance is surrounded by continuous accounting, automated systems, advanced analytics, data quality, and transactions. Hence, it is important to increase the protection of accounts to avoid fraud and threats online.

The banking industry, one of the subsets of the larger finance industry, adopted the use of one-time pins to authorize the user who performs an online transaction. According to Carstea (2024), technology has significantly changed users' expectations. The industry is prioritizing consumer needs through technology by eliminating complex processes that were previously used in traditional banking. Providing a secure experience is essential for establishing trust and loyalty. Users must feel confident in the security of their information as banks handle sensitive personal and financial data. Thus, features like one-time pins not only help prevent unauthorized transactions but also protect both the bank and its consumers. It serves as the user's key to their accounts, which helps prevent anyone but the user from making changes to the account. This feature helps in preventing certain kinds of online theft by ensuring that not only the pair of logged-in password and username is used to access the account. because it serves as an additional layer of protection against attackers. This is strong protection that provides safer use of e-wallets, online banking, and other systems that handle personally identifiable information. However, even if this authentication method can be said to be useful, it can still be said that it lacks security. The increasing number of identity thefts committed online shows that even one-time pins can still be stolen through deception.

Despite the widespread use of one-time pins as a security measure, previous research has focused on their effectiveness and vulnerabilities. However, there is still not much literature that explores user behavior and user experience in one-time pins that can provide an understanding of how users interact with one-time pin systems, such as their perceptions of OTP security, the influence of user fatigue, and how the OTP system is understood, which is still unexplored. This study aimed to fulfill this gap by determining if there is a difference between the users' perception and their demographic profiles, which will contribute as additional literature. Through this study, more information will be given to those who should improve OTP authentication systems, and this will give OTP users an idea of the experiences of other users.

2. LITERATURE REVIEW

A. One-Time Pin

The adoption of one-time pin (OTP) systems has significantly enhanced the security of online transactions in the digital age. One-time pins in reducing the risk of account takeover and unauthorized access adds extra layers of security to the authentication process, making it more secure and thwarting potential attackers' attempts to access sensitive information and also aids in preventing fraud and identity theft by verifying identities and authorizing users.

According to Richards and Wigmore (2021) one-time pins (OTPs) describe a security system that generates and delivers a random code to a user, serving as their temporary identity for online transactions, and the primary purpose of this code is to authenticate the user's identity and to confirm ownership of the account or transaction through a unique, time-sensitive token. Dynamic password authentication employs a One-Time Pin (OTP) in conjunction with a static password to verify users in two-factor authentication. Static passwords alone are susceptible to discovery and misuse by attackers.

In addition, Murcia (2023) claimed One-time pin's identity authentication aspect verifies the attempt to log in to a service for an online money transaction from their mobile cellular devices. Before the actual entry, the website or application system requests verification from the user to safeguard their information from unauthorized access or breach. The user's validation of its ownership allows them to continue going through different selections of receiving the one-time pin, which can be via text message, phone call, email, or push notification.

The one-time pin that has been delivered after the processing takes a short while, and after that, the user is capable of fully accessing them, continuing the online transaction, and freely acquiring many more sections of the service; and to guarantee that authorized users have permission to have access to sensitive data, a one-time pin provides a quick, safe, and effective means of user authentication. This procedure confirms that the person has access to both their phone and the right phone number which adds an additional degree of protection above and beyond the use of a login and password (Bhaat & Rai, 2023).

B. Online Transactions

According to Jain (2023), the implementation of one-time pins has proven to be an effective measure in preventing fraud by adding a crucial layer of identity verification during financial transactions. This system ensures that only the legitimate user can authorize payments, reducing the risks associated with unauthorized access to accounts. one-time pins are sent directly to the user's verified contact information, such as email or phone, ensuring the security of sensitive data during transactions.

The frequency with which consumers engage in online transactions is shaped by a multitude of factors, including perceived usefulness, user satisfaction, and individual demographic characteristics. Kazi (2013) asserts that the intention to adopt online banking is largely influenced by its perceived usefulness, credibility, and the convenience it offers users. This aligns with the findings of Kam and Riquelme (2007), who emphasize that while users appreciate the accessibility of online banking services, concerns regarding privacy and security can significantly affect their overall satisfaction and, consequently, their frequency of use.

As noted by Singer, Baradwaj, Flaherty, & Rugemer (2012), a user's experience can have a negative effect on the use of online banking, especially if it affects how easy and useful people believe the service to be. It is determined by the user's prior experience with online transactions and how frequently they use it. Highly educated individuals are more likely to choose online banking services.

While females are more likely to choose online banking services, individuals who are not working in the government sector are more likely to choose online banking services (Duasa, Nazri, & Zainal, 2019). Factors such as cognitions of financial advantage, perceived usefulness, platform

convenience, and platform risk significantly influence people's behavior towards online banking. Individual variables like gender, monthly income, and the platform used have a significant impact on people's behavior toward online banking (Zhan & Huang, 2019)

Generally, they collectively suggest that a variety of experiential and effectiveness factors influence the frequency of its users' online transaction use. The frequency of online transaction usage depends on the users' needs being satisfied by their experience. The users find online transactions useful as it offers convenience and maximizes effort to go to physical banks and stores only to keep on top of users' finances and be able to check account balances quickly, view transactions and know exactly what is going on with their accounts.

C. Security

Security mechanism is to verify users' identities, particularly in online transactions and account access. However, it's crucial to use strong passwords to safeguard the generation of one-time pins and to rely on trusted sources for implementing robust security measures to mitigate associated risks. Erdem & Sadikkaya (2019) assert that employing one-time pins in online transactions is a promising approach to enhancing security.

To strengthen the security of online transactions, the adoption of a one-time pin as a second-factor authentication method is widespread (Sharma & Nene, 2020). One-time pins provide an additional layer of security to the authentication process in online transactions.

When a user initiates an online transaction, the system prompts them to enter a one-time password generated by a one-time pin generator. This password is valid only for a single transaction and has a limited time frame, usually a few minutes.

Bhavsar, V., Kadlak, A., & Sharma, S. (2018) emphasize that user education plays a critical role in mitigating risks. To sum up, by teaching users how to identify phishing attempts, such as checking for suspicious URLs and verifying the sender's identity, they are less likely to fall prey to such attacks and they can recommend implementing two-factor authentication (2FA) to add an extra layer of protection.

D. Vulnerability

Kim & Yi (2023) observed that OTP systems rely on the randomness of generated numbers to enhance security, vulnerabilities often surface during the execution phase. Even with robust cryptographic methods in place, the application of OTPs can be exploited, diminishing user confidence in online financial systems. This highlights the need for continuous monitoring and improvement to address emerging threats.

In response to these vulnerabilities, Husain & Salman (2020) proposed an advanced approach to OTP security. Their research introduced multi-level encryption combined with the dual OTP technique, utilizing Blowfish and Advanced Encryption Standard (AES) algorithms.

This system offers increased protection against common attacks such as phishing and replay attacks, making it particularly suitable for online banking transactions. The dual OTP approach addresses the limitations of single-factor OTPs and significantly enhances transaction security.

Furthermore, Cagalj, Perković, & Bugarić (2015) focused on preventing timing attacks in OTP systems. Their study proposed incorporating randomness into the timing of OTP challenges and responses to obscure predictable patterns that attackers could exploit. Additionally, they suggested the use of masking techniques to reduce the cognitive load on users, thereby increasing the overall security and usability of OTP-based authentication.

II. METHODOLOGY

A. Research Framework

The research framework is illustrated in Figure 1. As framework presents the connection between the demographic profiles of respondents and the differences in group perspectives regarding their interactions with one-time pin. Progressing to evaluates level of technological proficiency to assess respondents' understanding and skill in using one-time pins. Ensuring the strength of security and vulnerability, the effectiveness of one-time pins, and identifies potential risks and challenges in using one-time pin for online transactions.

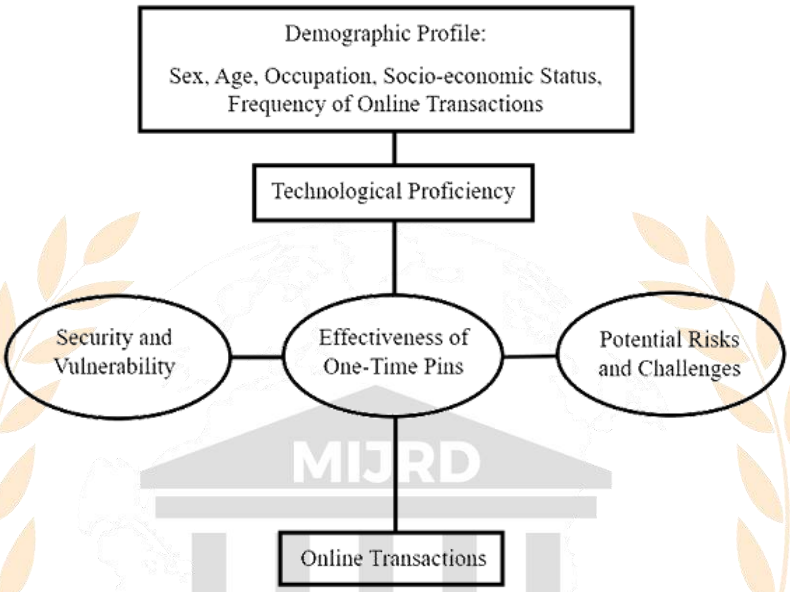
Demographic Profile:
Sex, Age, Occupation, Socio-economic Status, Frequency of Online Transactions
Technological Proficiency
Security and Vulnerability
Effectiveness of One-Time Pins
Potential Risks and Challenges
Online Transactions

Figure 01: Research Framework

B. Respondents

The respondents in the study are users of one-time pins for online transactions composed of employed and individuals from Mandaluyong City. The gathered information to be analyzed is based on their gender, age, occupation, socio-economic status and the frequency of using OTPs. Each data collected was through a physical meeting, where respondents completed the survey questionnaires on the spot. It was ensured that all respondents were verified as users of online transactions involving OTP. The participants were chosen using Purposive sampling, a non-probability-based technique recommended by Frost (2021). Purposive sampling was employed, selecting participants who met the specific criteria required for the study. The respondents were gathered in Mandaluyong City, resulting in a total of 180 participants.

C. Instruments

Demographic Profile

The independent variables, including gender, age, occupation, socio-economic status, and frequency of OTP use in online transactions in Mandaluyong City, help determine whether these factors influence users' differing opinions. Following Busayo (2021), respondents' age categories, rather than exact ages, were used for data segmentation, as grouping ages in 5- or 10-year intervals is more organized and effective. Socio-economic status was classified based on the Philippine Statistics Authority's 2021 Family Income and Expenditure Survey (FIES), which defines seven income categories, ranging from poor (below ₱12,030), low (₱12,030–₱24,120), lower middle (₱24,120–₱48,120), middle (₱48,120–₱84,210), upper middle (₱84,210–₱144,360), upper income (₱144,360–₱240,600), and rich (above ₱240,600).

Technological Proficiency Section

This parameter is a one-dimensional measure designed to assess respondents' technological proficiency in using one-time pins (OTPs) for online transactions. consists of five self-made items, validated by professionals to ensure reliability and validity of each question. It has been argued that midpoints in Likert scales can lead to unclear results, as respondents may select them to avoid engaging with the questions. To address this, a 4-point Likert scale was used, eliminating the midpoint and requiring respondents to take a definitive stance, as noted by Chyung, Roberts, Swanson, and Hankinson (2017). Respondents indicate their agreement with each statement by selecting the appropriate response from the 4-point Likert scale, where responses ranges from 1 is "Strongly Disagree" and 4 indicates "Strongly Agree". In estimating the level of technological proficiency, the researchers employed the following equivalences: "Beginner" corresponds to "Strongly Disagree", "Intermediate" to "Disagree", "Advanced" is "Agree", and "Expert" for the "Strongly Agree". Cronbach's alpha was calculated to be 0.81, exceeding the acceptable level of 0.60, suggesting that the instrument is reliable. Therefore, the researchers have confidence in the instrument's internal consistency and reliability for evaluating respondents' technological skills in employing one-time pins for online transactions.

Common Security and Vulnerability Section

Measuring the users' experiences with common security issues and vulnerabilities encountered when using one-time pins for online transactions. It comprises five self-developed question sets, carefully crafted and validated by experts to ensure the relevancy of each item according to specific parameters. The strongest items were refined to provide evidence for uncovering key insights into the security and vulnerability of OTP usage. Responses were measured on a 4-point Likert scale, ranging from 1 representing "Strongly Agree" to 4 representing "Strongly Disagree". Following reliability testing, the Cronbach's alpha coefficient was found to be 0.67. Although modest, it exceeds the acceptable threshold of 0.60 and demonstrates the adequate reliability.

Effectiveness of One-Time Pins Section

This instrument evaluates the effectiveness of one-time pins (OTP) in improving security and efficiency. Respondents will rate their level of agreement with each statement based on their experiences and beliefs, using a 4-point Likert scale, where 1 denotes "Strongly Disagree" and 4 denotes "Strongly Agree." The researchers developed five items for this scale, which were thoroughly tested for quality and context under the supervision of validators to confirm the accuracy of the questions. The instrument was subsequently evaluated for reliability to confirm that each statement met acceptable standards. The Cronbach's alpha coefficient was found to be 0.90, which exceeds the acceptable threshold of 0.60.

Risk and Challenges of Implementing One-Time Pins Section

The questionnaire examines the risks and challenges associated with implementing one-time pins (OTPs) as a security measure. Respondents rate their perceptions and experiences regarding various aspects of OTP implementation using a 4-point Likert scale, where 1 represents "Strongly Disagree" and 4 represents "Strongly Agree." Feedback from validators was used to enhance the questionnaire, specifically addressing the identified risks and challenges of OTP implementation. Following professional recommendations, the questionnaire was revised to mitigate these shortcomings. A reliability test was conducted with 30 one-time pin users to evaluate the contents under various conditions, confirming the accuracy of the five items in the final questionnaire. The Cronbach's alpha was 0.82, exceeding the acceptable threshold of 0.60.

D. Statistical Analysis

Statistical software Jamovi was utilized to evaluate the data. Percentage was used to show the proportion of the respondents with respect to their demographic characteristics. Weighted mean was used to determine the average level of response of the respondents' Common Security and Vulnerability Problems, Effectiveness of One-time pin in preventing unauthorized access and fraudulent activities during Online Transactions, and Potential risks and challenges of implementing One-time pins for accessing sensitive data during online transactions. Mann-Whitney U-test / Kruskal-Wallis H-test were used to evaluate the differences of respondents' perspectives on common security and vulnerabilities associated with one-time pins and respondents' perspective on the effectiveness of one-time pins in preventing unauthorized access and fraudulent activities during online transactions are different from their demographic profile.

III. RESULTS

Table 1: Distribution of Respondents' Demographic Profile

Demographic Profile		Frequency (N)	Percentage (%)
Sex	Male	76	42%
	Female	104	58%
Age	18-24	39	22%
	25-35	74	41%
	36-45	45	25%
	46-60	22	12%
Occupation	Health	16	9%
	Finance	22	12%
	Technology	26	14%
	Education	38	21%
	Retail	14	8%
	Manufacturing	8	4%
	Food	26	14%
	Other	30	17%
Socio-Economic Status	Less than 12,030 Php	23	13%

Volume: 04 / Issue: 03 / 2025 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

	Between 12,030 to 24,120 Php	52	29%
	Between 24,120 to 48,120 Php	73	41%
	Between 48,120 to 84,210 Php	23	13%
	Between 84,210 to 144,360 Php	5	3%
	Between 144,360 to 240,600 Php	4	2%

The demographic profile of respondents shows that sex consists of 76 (42%) males and 104 (58%) females, indicating a slight majority towards female representation. Given the instances in which some men were unavailable in the sample due to factors such as lack of time, being qualified but unemployed, or qualified but not using online transactions.

In terms of age, most of the respondents fall within the age ranges of 25 - 35 years old with a total of 74 or 41%, followed by 36 to 45 years old, accounting for only 25%. Respondents aged 18 to 24 years contributed 39 responses, representing 22% of the total. The age group of 46 to 60 years exhibited the lowest participation, with 22 respondents comprising 12% of the sample. This indicates that individuals between the ages of 25 and 35 are increasingly adopting online transactions.

When it comes to occupation, a huge portion of respondents are employed in the education sector, 38 individuals (21%). This suggests that individuals from the education sector frequently engage in online transactions. Followed by 30 or 17% of respondents who fall into the "other" category, indicating a range of professions not covered by the predefined categories, reflecting the population's occupational diversity. Moreover, both technology and food service had the same result of respondents of 26 or 14%. The finance sector registered 22 respondents (12%), while the healthcare sector accounted for 16 respondents (9%). Retail recorded 14 respondents (8%), and manufacturing with 8 respondents (4%).

Lastly, in socio-economic status, the lowest number of respondents belong to the upper income category Between 144,360 to 240, 600 Php (4 or 2% of the total respondents), followed by upper middle income Between 84,210 to 144,360 Php with only 5 respondents (3%). Poor or less than 12,030 Php and middle income between 48, 120 to 84,210 Php had the same number of respondents with a total of 23 or 13% respondents. In contrast, the highest percentage of respondents earned is lower middle-income between 24,120 to 48,120 Php with a total of 73 or 41%. And lastly, the lower middle income earned between 12,030 to 24,120 Php with 52 (29%) respondents. This helps to highlight how the digital divide can potentially hinder online transactions by using this distribution table. That is why socioeconomic status should be understood because it can help assess the effectiveness of security measures such as one-time pins in different socioeconomic contexts, which can lead to important findings.

Table 2: Frequency of Online Transactions

Frequency of Online Transaction	Frequency (N)	Percentage (%)
Daily	59	33%
Weekly	56	31%

Monthly	40	22%
Rarely	25	14%

The frequency of respondent's online transactions displays a significant portion of 59 individuals (33%), engaging in daily transactions, indicating a high level of comfort and regularity. Weekly transactions are conducted by 56 respondents (31%), while 40 respondents (22%) transact monthly, showing periodic engagement. The lowest activity level is seen among 25 users (14%), who engage less frequently. Overall, these findings highlight the increasing reliance on digital payment methods, reflecting a broader societal shift toward digital financial operations.

Table 3: Respondents' Level of Technological Proficiency

Parameter	Weighted Average	VI
Technological Proficiency	3.44	Advanced

The level of technological proficiency of the respondents revealed an overall weighted average of 3.44, corresponding to an advanced performance level. The weighted average value of 3.44 further explains that the respondents demonstrate a strong proficiency in handling one-time pin-related tasks. This score reflects a high level of comfort and capability in using various devices and platforms that require one-time pins, as well as familiarity with potential security risks and technical issues.

Table 4: Perceived Common Security and Vulnerability Problems Associated Using One-Time Pin in Online Transaction

Parameter	Demographic Profile		Weighted Average	VI
Common Security and Vulnerability	Sex	Male	3.31	Agree
		Female	3.30	Agree
	Age	18-24	3.31	Agree
		25-35	3.30	Agree
		36-45	3.31	Agree
		46-60	3.20	Agree
	Occupation	Healthcare	3.40	Agree
		Finance	3.47	Agree
		Technology	3.22	Agree
		Education	3.38	Agree
		Retail	3.00	Agree
		Manufacturing	3.30	Agree
		Food	3.35	Agree
		Other	3.22	Agree

	Socio-Economic Status	Less than 12,030 Php	3.25	Agree
		Between 12,030 to 24,120 Php	3.27	Agree
		Between 24,120 to 48,120 Php	3.35	Agree
		Between 48,120 to 84,210 Php	3.24	Agree
		Between 84,210 to 144,360 Php	3.56	Agree
		Between 144,360 to 240,600	3.45	Agree

Common security and vulnerability of one-time pin (OTP) in online transactions identify potential differences in opinions, highlighting between males and females through the analysis of survey response means. The average weighted mean scores of 3.31 (Agree) for male respondents and 3.30 (Agree) for female respondents indicate that, despite gender differences, both groups hold similar views regarding the security measures and vulnerabilities associated with OTPs. Indicating that these concerns are widely recognized across genders.

The questionnaire results demonstrate that respondents between 18-24 years old have an average weighted mean of 3.31 (Agree), while those aged 25-35 have a mean of 3.30 (Agree). Participants in the 36-45 age group reported a mean of 3.36 (Agree), and those between 46-60 years old recorded a mean of 3.20 (Agree). All age groups hold similar views on the security of one-time pins and generally agree on the vulnerability factors outlined in the survey based on their experiences.

Meanwhile, occupation has the Finance sector achieved the highest overall weighted mean of 3.47 (Agree), followed by healthcare at 3.40 (Agree) and education at 3.38 (Agree). The food industry recorded a mean of 3.35 (Agree), while manufacturing had a mean of 3.30 (Agree). Both the technology sector and the category "others," encompassing specified jobs outside the latter industries, each obtained a mean of 3.22 (Agree). Retail had the lowest average weighted mean at 3.00 (Agree). Regardless of their professions, acknowledged the effectiveness of one-time pins as a security measure for online banking platforms. However, their vulnerabilities to attacks, potential delays, and susceptibility to scams underscore the importance of understanding their limitations.

Lastly, socio-economic status, respondents in the poor that earn less than 12,030 Php category have an average weighted mean of 3.25 (Agree), while those in the low category earning between 12,030 to 24,120 Php average 3.27 (Agree). Respondents from the lower middle earning between 24,120 to 48, 120 Php category achieve a mean of 3.35 (Agree), and those in the middle-middle, between 48, 120 to 84,210 Php category show a mean of 3.24 (Agree).

In contrast, respondents from the upper middle category in between 84,210 to 144,360 Php demonstrate strong agreement with an average weighted mean of 3.56 (Strongly Agree), while the upper income category who has been earning between 144,360 to 240, 600 Php shows agreement with a mean of 3.45 (Agree). This highlights the significance of the questions in shaping perceptions, as upper middle income users of one-time pins demonstrate strong confidence in the questionnaire's relevance to their personal experiences and concerns.

Table 5: Differences in the Respondents' Perspective of the Common Security and Vulnerabilities Associated Using One-Time Pin in Online Transactions when Grouped by Profile

Demographic Profile	Computed U/H Value	P-Value	Decision	Remarks
Sex	3871	0.877	Failed to reject H0	Not Significant
Age	4.02	0.638	Failed to reject H0	Not Significant
Occupation	5.37	0.104	Failed to reject H0	Not Significant
Socio-Economic Status	2.46	0.830	Failed to reject H0	Not Significant

The differences in respondents' perspectives on the common security and vulnerabilities associated with using one-time pins (OTP) in online transactions when grouped by demographic profile. Results show no statistically significant impact of demographic profiles on respondents' perceptions of one-time pins security and vulnerability. Since, all p-values are greater than 0.05. Specifically, sex (P = 0.877), age (P = 0.638), occupation (P = 0.104), and socio-economic status (P= 0.830). Therefore, the null hypothesis is accepted, indicating no significant differences in respondents' perceptions of OTP security across demographic profiles.

Table 6: Perceived Effectiveness of One-Time Pin in Preventing Unauthorized Access and Fraudulent Activities During Online Transactions

Parameter	Demographic Profile		Weighted Average	VI
Effectiveness of Using One-Time Pin	Sex	Male	3.36	Agree
		Female	3.35	Agree
	Age	18-24	3.39	Agree
		25-35	3.39	Agree
		36-45	3.35	Agree
		46-60	3.14	Agree
	Occupation	Healthcare	3.38	Agree
		Finance	3.48	Agree
		Technology	3.39	Agree
		Education	3.28	Agree
		Retail	3.06	Agree
		Manufacturing	3.23	Agree

		Food	3.47	Agree
		Other	3.32	Agree
	Socio-Economic Status	Less than 12,030 Php	3.42	Agree
		Between 12,030 to 24,120 Php	3.39	Agree
		Between 24,120 to 48,120 Php	3.31	Agree
		Between 48,120 to 84,210 Php	3.33	Agree
		Between 84,210 to 144,360 Php	3.40	Agree
		Between 144,360 to 240,600	3.10	Agree

This provides an analysis of respondents' perceptions of the effectiveness of one-time pins (OTPs) in preventing unauthorized access and fraud during online transactions, categorized by demographic profile.

Across all groups, respondents generally agree on the usefulness of one-time pins, with slight variations in their weighted averages.

Sex, both males (3.36) and females (3.35) exhibit similar agreement levels, indicating a shared perception of one-time pin effectiveness between sex. When it comes to age, those between 18-24 and 25-35 years old, express the strongest agreement (3.39) while ages 46-60 years old, show slightly lower levels of agreement (3.14), possibly that older users may have more difficulty with or lower trust in OTP systems.

In occupation, the finance sector shows the highest confidence in OTPs with a weighted average of 3.48, followed closely by the food industry of 3.47 weighted average and technology (3.39). This could be due to these sectors being more familiar with or reliant on secure online transactions.

Meanwhile, those in retail (3.06) and manufacturing (3.23) show the lowest agreement, which may indicate less frequent exposure to OTPs or a perception that they are less necessary in their respective industries.

For socio-economic status, respondents belonging to the poor who earned less than 12,030 Php (3.42) demonstrate the highest confidence in one-time pins, followed by the upper middle class earning Between 84,210 to 144,360 Php (3.40), while those with the highest income between 144,360 and 240,600 Php or the upper class (3.10) report the lowest agreement.

This may reflect a difference in the perceived necessity or trust in one-time pins between lower and higher-income individuals, with wealthier respondents possibly having access to alternative security measures.

Table 7: Differences in the Respondents' Perspective of the Effectiveness of One- Time Pin in Preventing Unauthorized Access and Fraudulent Activities During Online Transactions when Grouped by Profile

Demographic Profile	Computed U/H Value	P-Value	Decision	Remarks
Sex	3581	0.711	Failed to reject H0	Not Significant
Age	5.03	0.516	Failed to reject H0	Not Significant
Occupation	5	0.338	Failed to reject H0	Not Significant
Socio-Economic Status	1.27	0.836	Failed to reject H0	Not Significant

Analyzing the effectiveness of one-time pins (OTPs) in preventing unauthorized access and fraud during online transactions, considering demographic differences. The computed U and H test values, along with p-values starting with sex (P = 0.711), age (P = 0.513), occupation (P = 0.338) and socio-economic status (P = 0.836) reveal no significant differences in respondents' views as the p-value exceeds 0.05. Contributing to the remarks of insignificant results due to the failure to reject the null hypothesis.

Table 8: Perceived Potential Risks and Challenges of Implementing One-Time Pins for Accessing Sensitive Data During Online Transactions

Parameter	Weighted Average	VI
Risk and Challenges of Implementing OTP	3.23	Advanced

A moderate number of respondents expressed agreement regarding the risks and challenges associated with the implementation of one-time pins (OTP), as reflected by an average weighted mean of 3.23 from the five-item questionnaire. Their concerns highlight the vulnerability of OTPs, particularly during operation, where potential breaches or compromises could occur, posing significant risks to digital security protocols.

IV. DISCUSSION AND CONCLUSION

Respondents are highly involved in online transactions, and most of them view OTPs as an effective security measure. The majority of respondents indicated that they conduct online transactions on a daily or weekly basis, and diverse demographic groups agreed that OTPs are useful in preventing unauthorized access.

Although satisfaction differs depending on demographic profile, some users are concerned about security, inconvenience, and phishing threats.

Weighted averages across demographic groups show that most people understand the importance of strong OTP security, but some are concerned about problems with security. The statistical analysis shows that demographic profiles had no significant impact on perceptions of OTP effectiveness and associated vulnerabilities. This suggests that users across various groups generally have similar perceptions of OTPs, even though they have specific concerns regarding their security.

Furthermore, respondents recognize the importance of OTPs in online transactions; however, addressing their vulnerabilities is crucial for increasing user confidence. Which is consistent with previous research by Si, Sharma, and Ye Wang (2024), who highlighted the importance of user education in reducing perceived risks associated with digital security measures.

In conclusion, this study found that respondents perceived OTP as a generally effective feature, with no statistically significant differences observed in the perceptions of demographic groups. Thus, in order to optimize the effectiveness of OTPs in online transactions, efforts must be made to address security concerns even as users understand the benefits and importance of OTPs.

RECOMMENDATION

The findings emphasize the importance of raising user awareness about online data security, particularly when using one-time pins (OTPs) for transactions. This knowledge will help users understand potential issues and adopt cautious practices to mitigate risks, thereby securing their online interactions. Companies engaged in online banking and digital transactions should prioritize the enhancement of security measures in line with the study's findings. Future researchers are encouraged to conduct broader investigations using diverse methods, such as qualitative interviews, to uncover new insights. Continuous improvements to OTP systems are vital to counter evolving cyber threats and prevent unauthorized access and fraud. Readers are urged to leverage this study to deepen their understanding of cybersecurity practices, remain vigilant against emerging threats, and consider implementing multi-factor authentication methods. Respondents emphasized the necessity for stronger security protocols, suggesting that companies integrate additional user-specific authentication methods, including Dynamic Pin Lengths and Characters, Geolocation Verification, and Personalized OTP Generation, to significantly fortify platform security and reduce the risk of cyber threats.

REFERENCES

[1] Bhaat, S., & Rai, N. (2023). Using SMS OTP For Enhanced Security

[2] Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. International Journal of Computer Applications, 182(33), 27–29. https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks

[3] Busayo, L. (2021). Age Survey Questions: How to Classify Age Range or Groups. Formplus Blog. https://www.formpl.us/blog/age-survey-questions

[4] Cagalj, M., Perkovic, T., & Bugaric, M. (2015). Timing Attacks on Cognitive Authentication Schemes. IEEE Transactions on Information Forensics and Security, Vol.10, no.3, pp.584–596. https://doi.org/10.1109/tifs.2014.2376177

[5] Carstea, D. (2022). 5 Ways the Banking & Financial Sectors Have Adapted To Technology. Stefanini. https://stefanini.com/en/insights/articles/5-ways-banking-financial-sectors-have-adapted-to-technology

[6] Chyung, S. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence- Based survey design: The use of a midpoint on the likert scale. Performance Improvement, 56(10), 15–23. https://doi.org/10.1002/pfi.21727

[7] Duasa, J., Nazri, N. J. Z., & Zainal, N. H. (2019). Likelihood of using online banking services among consumers: application of logit model. Typeset.io. https://www.semanticscholar.org/paper/Likelihood-of-using-online-banking-services-among-Duasa-Nazri/a3f2e69e0f86ccb2de253410f13a12835272fa78

[8] Erdem, E., & Sandikkaya, M. T. (2019). OTPaaS—One Time Password as a Service. IEEE Transactions on Information Forensics and Security, Vol.14, No.3, pp.743–756. https://doi.org/10.1109/tifs.2018.2866025

[9] Frost, J. (2021). Purposive Sampling: Definition & Examples. Statistics by Jim. https://statisticsbyjim.com/basics/purposive-sampling/

[10] Jain, P. (2023). What is OTP in Credit Card Transactions? My Money Mantra. https://www.mymoneymantra.com/blog/what-is-otp-in-credit-card-transactions

[11] Kam, B. H., & Riquelme, H. (2007). An Exploratory Study of Length and Frequency of Internet Banking Usage. Journal of Theoretical and Applied Electronic Commerce Research, Vol.2, No.1, pp.76–85. https://doi.org/10.3390/jtaer2010007

[12] Kazi, A. (2013) An empirical study of factors influencing adoption of Internet banking among students of higher education: Evidence from Pakistan. MPRA Paper; University Library of Munich, Germany. Vol.2, No.2, pp.2147–4486. https://ideas.repec.org/p/pra/mprapa/48611.html

[13] Kim, H., & Yi, O. (2023). Analysis of Distinguishable Security between the OneTime Password Extraction Function Family and Random Function Family. Applied Sciences, Vol.13, No.15, pp.8761. https://doi.org/10.3390/app13158761

[14] Murcia, A. (2023). What is a one-time password (OTP)? Features and benefits explained. Sinch. https://www.sinch.com/blog/one-time-password/

[15] Philippine Statistics Authority. (PSA) (2021). SA Approves the Conduct of the 2021 Family Income and Expenditure Survey (FIES). https://www.psa.gov.ph/content/psa-approves-conduct-2021-family-income-and-expenditure-survey-fies

[16] Richards, and Wigmore. "What Is a One-Time Password (OTP)? Definition from SearchSecurity." SearchSecurity, Sept. 2021, www.techtarget.com/searchsecurity/definition/one-time-password-OTP.

[17] Husain, & Salman, M. (2020). A Review of Information Security from Consumer's Perspective Especially in Online Transactions. Social Science Research Network, Vol.10, No.4, pp.11–14. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3669577

[18] Sharma, M. K., & Nene, M. J. (2020, January 12). Two-factor authentication using biometric based quantum operations. Wiley Online Library. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.10

[19] Singer, D., Flaherty, S., Baradwaj, B. G., & Rugemer, F. (2012). Journal of Internet Banking and Commerce. The Frequency and Intensity of Experience in Online Banking Use, 17(1). https://www.icommercecentral.com/open-access/the-frequency-and-intensity-of-experience-in-online-banking-use.pdf

[20] Sutton, N. (2023). The Role of Technology in the Finance Industry. Advanced. https://www.oneadvanced.com/news-and-opinion/the-role-of-technology-in-the-finance-industry/#:~:text=Technology%20has%20completely%20transformed%20how

[21] Zhan, J., & Huang, W. (2019). People's Behavior of Online Banking and its Influencing Factors. Typeset.io, Vol.1, pp.229–234. https://doi.org/10.35532/JSSS.V1.047