ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available online at: https://www.ijergs.in

Volume - 11, Issue - 6, November – December – 2025, Page No. 28 – 36

Understanding mobile device vulnerability to phishing

[1]Chahat Jayant, [2]Riya Kumari, [3]Kartik Yadav, [4]Shreya Rai, [5]Ayush Kumar, [6]Dr. Naveen Kumar Sharma

[1-6]Department of Department of MCA, IIMT College of Engineering, Greater Noida.

Abstract

The mobile device is one of the fasted growing technologies that is widely used in a diversifying sector. Mobile devices are used for everyday life, such as personal information exchange – chatting, email, shopping, and mobile banking, contributing to information security threats. Users' behavior can influence information security threats. More research is needed to understand users' threat avoidance behavior and motivation. Using Technology threat avoidance theory (TTAT), this study assessed factors that influenced mobile device users' threat avoidance motivations and behaviors as it relates to phishing attacks. From the data collected from 137 mobile device users using a questionnaire, the findings indicate that (1) mobile device users' perceived susceptibility and severity of phishing attacks have a significant correlation with a users' perception of the threat; (2) mobile device users' motivation to avoid a threat is correlated to a users' behavior in avoiding threat; and (3) a mobile device user's susceptibility to phishing attacks can be reduced by their perception of the threat. These findings reveal that a user's perception of threat increases if they perceive that the consequence of such threat to their mobile devices will be severe, thereby increasing a user's motivation and behavior to avoid phishing attack threats. This study is beneficial to mobile device users in personal and organizational settings.

Keywords: Phishing Attacks, Security Behavior, Technology Threat Avoidance, Avoidance Motivation, Mobile Device Users' Security Behaviour.

Introduction

Mobile devices now perform as personal computers instead of a communication device as technological and computing capabilities increase. Mobile devices are used to perform everyday interactions and transactions and have contributed to increased security concerns for users. Security threats are increasing as the global population continues to adopt mobile device use. Phishing attackers continue to look for ways to penetrate mobile devices [1] [2]. As users' dependence on mobile devices increases, so is their susceptibility to information technology threats. Therefore, it has become necessary to understand the avoidance motivation and behavior of users. It is important to understand mobile device user behaviors as their dependency on mobile devices increases [3].

Mobile device users are more susceptible to phishing attacks than desktop users [4]. Some mobile device users are not aware of phishing attack techniques and may not realize that they are victims or could become victims of an attack [5] [6]. [7] pointed out the differences in how users interact with computers compared with mobile devices impact vulnerabilities. Users can perform only a subset of activities on their mobile devices and, due to the portable size of their mobile devices, may miss some vital details and click on or open malicious emails. For example, mobile device users may more frequently focus on urgency cues in email and omit unconventional grammar or spelling in emails than computer users, thus increasing the possibility of being a victim of phishing attacks [8]. A change in mobile device users' behavior can reduce the victimization of phishing attacks [9]. Despite the recent increase in attention on IT

security driven by the pervasiveness of technology in human interactions, there is a need for research on the impact human behavior has on cybercrime vulnerabilities in the context of mobile devices [10].

Even though mobile devices are one of the fastest-growing markets in the technology sector, there has been limited research done to understand why mobile device users are increasingly falling victims to phishing attacks. Thus, it is essential to understand mobile device users' perspectives on avoiding phishing attacks and how they might be protected from internet security threats while using their devices. Incorporating human behavior into our understanding of mobile device vulnerabilities will aid in the development of the next generation of mobile device security tools and strategies.

Recent research has detailed the growing threat to mobile device security [11], [12]. However, most of these studies focus on mobile vulnerability analysis to internet threats [13], online security tools to thwart IT threats, and malware and phishing attacks concerning websites or URLs [7]. Malware and phishing studies on mobile devices focus on the growing trend of sophisticated malware [14] and techniques to detect phishing attacks and countermeasures [15]; Security studies of mobile applications focus on areas such as spoofing with the use of malicious applications [12]. Several studies note that the increased dependence on mobile devices is concurrent with an increase in users' vulnerability to phishing attacks [16], [3]. Studies on online security tools focus on protecting users from IT threats [17], while a few studies combine mobile device users' avoidance behavior and their susceptibility to phishing attacks.

Although many studies indicate that internet security is a significant concern due to the increased use of mobile devices, there is little available information about mobile device users' perception of phishing attacks as an IT threat. Furthermore, research has not adequately addressed mobile devices users' security behavior in responding to phishing attacks [10]. It is necessary to understand why mobile device users are increasingly falling victim to phishing attacks or online threats [18]. This study examined the factors that make mobile device users susceptible to phishing attacks [7], [3], [4], user avoidance behavior, and motivation to avoid IT threats. In doing so, this study contributes to the body of research used to inform and update mobile device security practices.

The Present Study

The increased reliance on mobile devices can lead to an increased frequency of phishing attacks [19]. Exploring mobile device users' susceptibility to phishing attacks provides scholars and mobile device users with a better understanding of why preventive measures by themselves do not adequately protect against internet attacks. Such insights could help reduce the risky behavior of mobile device users and thereby thwart phishing attacks.

The study intended to investigate mobile device users' susceptibility to phishing attacks and provide insights into reducing users' risky behavior. This study aimed to inform scholars and individuals on a better understanding of internet threat behavior among mobile device users and preventive actions utilizing the technology threat avoidance theory (TTAT). TTAT explores the influence of perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior [10] on mobile device users' security behavior related to phishing attacks. By using the constructs outlined in TTAT [10], the research presented in this study addresses some of the gaps reported in the literature concerning IT threats. A better understanding of mobile device users' perception and behavior of the phishing attack might lead to a better approach in thwarting phishing attacks. Mobile

devices have many of the same capabilities as a laptop or personal computers and are therefore vulnerable to computer security threats. These computer threats are increasing in sophistication and complexity, regardless of the targeted device [18]. The results of this research could help users and practitioners move closer to their shared goal of decreasing mobile device threat vulnerabilities.

The remainder of the paper is organized into five remaining sections. Section 2 provides a comprehensive literature review, including a theoretical foundation and review of related studies. In Section 3, the study details the research methodology, population and sample, research design, instruments, and demographic characteristics used in this study. Section 4 provides an in-depth analysis of the data and the results. Research discussion, limitations, implications, and further research direction are discussed in Section 5; lastly, Section 6 details the conclusion of this study.

Research Methodology

This study utilized the technology threat avoidance theory (TTAT; [10]) to test the correlation between perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, avoidance behavior, and the mobile device users' security behavior as they relate to phishing attacks. The study addresses a new area of research on what motivates mobile device users to avoid phishing attacks [7]. There has been significant scholarly interest in the correlation between mobile device use and attacks [57]. The results of this study provide scholars and practitioners a new angle on understanding how the behavior of mobile device users impacts the success and frequency of phishing attacks [7].

Research Question and Hypotheses

This study examined, to what extent, if any, do the eight elements of the TTAT (perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self- efficacy, avoidance motivation, and avoidance behavior) influence mobile device users' susceptibility to phishing attacks. Eight research questions (RQ) directly follow:

1. To what extent does perceived severity influence mobile device users' susceptibility to phishing attacks?
2. To what extent does perceived susceptibility influence mobile device users' susceptibility to phishing attacks?
3. To what extent does perceived threat influence mobile device users' susceptibility to phishing attacks?
4. To what extent does safeguard effectiveness influence mobile device users' susceptibility to phishing attacks?
5. To what extent does safeguard cost influence mobile device users' susceptibility to phishing attacks?
6. To what extent does self-efficacy influence mobile device users' susceptibility to phishing attacks?
7. To what extent does avoidance motivation influence mobile device users' susceptibility to phishing attacks? And
8. To what extent does avoidance behavior influence mobile device users' susceptibility to phishing attacks?

These eight research questions were used to generate nine working hypotheses based on the TTAT constructs.

Hypothesis 1a. Mobile device users perceived susceptibility of being attacked by phishing has a positive relationship with their perception of threats.

Hypothesis 1b. Mobile device users perceived severity of being attacked by phishing has a positive effect on perceived threat. Hypothesis 1c. Mobile device users perceived susceptibility and perceived severity of a phishing attack have a positive interaction effect on perceived threat.

Hypothesis 2. Perceived threat from mobile device users positively affects user's avoidance motivation.

Hypothesis 3: Safeguard effectiveness against phishing attacks positively affects avoidance motivation.

Hypothesis 3a: Perceived threat of phishing attacks and safeguard effectiveness against phishing have a negative interaction effect on avoidance motivation.

Hypothesis 4: Safeguard cost against phishing attacks negatively affects avoidance motivation.

Hypothesis 5: Self-efficacy for taking safeguard measures against phishing attacks positively affects avoidance motivation.

Hypothesis 6: Avoidance motivation positively affects the avoidance behavior of using safeguard measures.

Population and Sample

The population for this study was mobile device users who own a mobile device and are age 18 and older living within the United States. Surveys were administered online and resulted in a demographically diverse sample population, an expected result due to the extensive use of mobile devices in the United States. The Pew Center reported that over 60% of adults use a mobile device to access the internet, and 15% of young adults ages 18-29 rely heavily on their smartphones for online access (as cited in [3]). There is a possibility that participants had limited or no knowledge about phishing attacks, which would yield a range of variance in the TTAT constructs measured by the survey, and this variance will be used to detect moderation effects.

The demographic for this study is diverse; participants include males and females who were 18 years and older, accessed the internet with their mobile devices, and completed a web-based survey.

Size and Power

This study examined the data for incomplete surveys, missing survey responses, and outliers. The total participants were N = 137, and eight cases were eliminated due to missing data leaving N =

129. This study used regression analysis, and assumption testing was performed to ensure that regression analysis was appropriate. For this study, Hypothesis 1a, Hypothesis 1b, Hypothesis 2, Hypothesis 3, Hypothesis 4, Hypothesis 5, and Hypothesis 6 were tested using simple linear regression, while Hypothesis 1c and Hypothesis 3a were tested using multiple linear regression. The minimum sample size for this study was N = 107, using G*Power 3.1.9.2, a power analysis program used in research studies including behavioral studies [58]. The power analysis confirmed 107 samples is appropriate for the study where alpha = .05, power (1 - β err prob) = .95, and effect size = .15. However, QuestionPro collected a random sample size of 137. There were eight missing data, thus, removed from the sample collected. After removing the eight missing data and six outliers, the sample size was N = 123.

Demographic Description

Participants for this survey were asked to provide their age group, gender, and education level. Of the 129 participants that completed the survey, 27.13% were between the ages of 18 and 25, 45.74% were between the ages of 26 and 40, 9.30%

were between the ages of 41 and 55, and 17.83% were 56 and older. The highest participants were in the 26-40 age group with N = 59 (45.74%), followed by the 18-25 age group represented by N = 35 (27.13%), as shown in Figure 1.

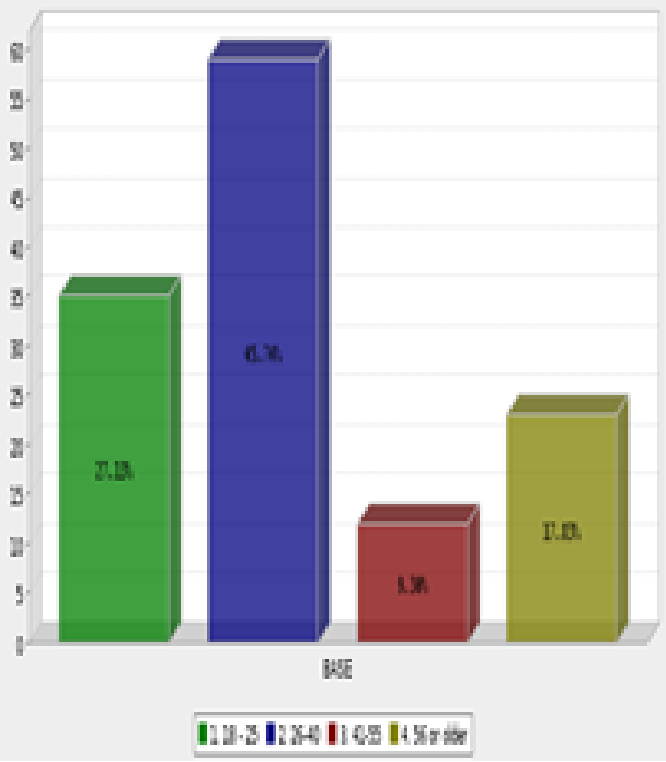

Figure 1: Participants' age group

Figure 2 shows that most participants were females with N = 88 (68.22%). The male participants were at least 50% less than the female participants. The male participants were N = 41 (31.78%) of the sample.

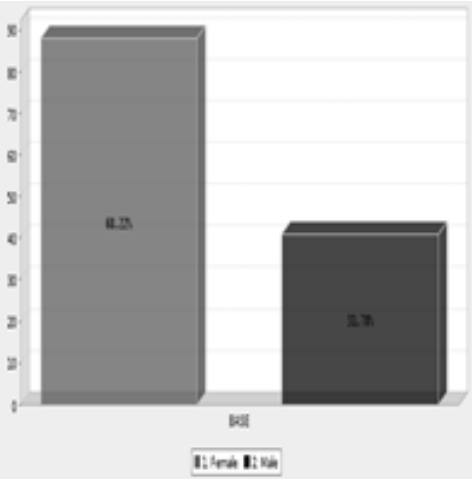

Figure 2: Gender of participants' sample

Participants of the study have attained some level of education. The education level of the participants that completed the survey includes a more significant number of those with some college level of education, with N = 44 (34.11%), followed by those with a high school or equivalent education level, with N = 41 (31.78%). Table 1 reflects the analysis of the education level for the participant.

Table 1: Frequencies of Participants by Education Level.

Hypothesis		Statistics	Findings
H1a	Mobile device users' perceived susceptibility of being attacked by phishing positively affects their perception of threat.	$F(1, 121) = 69.4$, $p < .001$	Supported
H1b	Mobile device users' perceived severity of being attacked by phishing positively affects their perception of threat.	$F(1, 121) = 379.6$, $p < .001$	Supported
H1c	Perceived susceptibility and perceived severity of a phishing attack have a positive interaction effect on perceived threat.	$F(2, 120) = 226.98$, $p < .001$	Supported
H2	Perceived threat of being phished positively affects avoidance motivation.	$F(1, 121) = 132.06$, $p < .001$	Supported
H3	Safeguard effectiveness against phishing attacks positively affects avoidance motivation.	$F(1, 121) = 183.26$, $p < .001$	Supported
H3a	Perceived threat of phishing attack and safeguard effectiveness against phishing has a negative interaction effect on avoidance motivation.	$F(2, 120) = 97.10$, $p < .001$	Supported
H4	Safeguard cost against phishing attacks negatively affects avoidance motivation.	$F(1, 121) = 21.21$, $p < .001$	Supported
H5	Self-efficacy for taking safeguard measures against phishing attacks positively affects avoidance motivation.	$F(1, 121) = 138.32$, $p < .001$	Supported
H6	Avoidance motivation positively affects the avoidance behavior of using safeguard measures.	$F(1, 121) = 134.40$, $p < .001$	Supported

Table 2: Summary of findings.

Education Level	Frequency	Percentage
High school or equivalent	41	31.78%
Vocational/technical school	6	4.65%
Some college	44	34.11%
Bachelor's degree	25	19.38%
Graduate school	13	10.08%
Other	0	0.0%

Table 3 provides the model summary of the nine dependent variables. This study conducted a regression analysis after confirming the homoscedasticity and normality of the residuals. The study met all regression assumptions. However, the Durbin-Watson value on avoidance motivation had a lower value. Six participants were outliers and were removed from the analysis. Hypothesis 1a, 1b, 1c, 2, 3, 3a, 4, 5, and 6 were all supported based on the statistical testing.

Table 3: Model Summary.

Variables	R	R^2	Adjusted R^2	Standard Error	Durbin- Watson
Perceived Susceptibility	.604	.364	.359	1.279	1.588
Perceived Severity	.871	.758	.756	0.789	2.271
Perceived Susceptibility and Severity	.889	.791	.787	0.737	1.868
Perceived Threat	.722	.522	.518	1.219	2.007
Safeguard Effectiveness	.776	.602	.599	1.112	1.779
Safeguard Effectiveness, Perceived Threat	.786	.618	.612	1.094	1.809
Safeguard Cost	.386	.149	.142	1.626	1.658
Self-Efficacy	.730	.533	.530	1.204	1.799
Avoidance Motivation	.725	.526	.522	1.363	1.381

Discussion

The primary aim of the present study was to explore mobile device users' susceptibility to IT threats such as phishing attacks and how motivated users were to avoid such threats. Phishing attacks are a popular means of attaining personal information by cybercriminals for fraudulent use, and it is necessary to understand how to mitigate these attacks most effectively [62]. The study presented here drew on TTAT to investigate how mobile device user behavior impacted the phishing attack landscape. The TTAT is a model used to examine IT threats avoidance and users' behavior given safeguard measures [29].

Implications for Practice

This study examines user IT threat avoidance behavior in the context of mobile devices because of their increased vulnerability to phishing attacks. In 2012, 99% of malware detection targeted Android devices – a form of a mobile device; malware attacks have dominated these devices [63]. In organizations, employees often receive training in security awareness, and they understand their accountability of behavior towards IT security [64]. Security policies are implemented and mandated in organizations, which in turn has attracted more information security research [65]. However, mobile device users are often not mandated by any organizational policies and can be victims of IT threats because they become prey. Anti-phishing applications were developed to thwart phishing and provide awareness to users about phishing attacks [29] but are not sufficient to thwart phishing attacks [66], [6] on mobile devices.

This research indicates that consumers' perception of threat best predicts 52.2% of phishing attack avoidance motivation. As indicated by the results, consumers' perception of threat will increase if they perceive that the consequences of the threat to their mobile device will be severe. The indicated result may encourage users to increase self-efficacy and adopt safeguard measures on their mobile devices. Thus, using safeguard measures on mobile devices could be increased based on their motivation to avoid phishing attacks. To reduce phishing attacks and increas

Research Limitations and Future Research

Though designed to be generalizable, this study had several limitations. While power analysis indicated that the sample size would be enough to detect statistical significance, this study was limited to a small number of participants that may not understand the meaning of phishing. Before taking the survey, there was no explanation of phishing given to the participants, leaving the possibility that the participants responded to the survey without explicit knowledge of phishing attacks. On the other hand, prior knowledge about phishing attacks could have impacted the data and the analyses of the results.

Another limitation is the length of the survey. The survey consisted of 44 questions which could pose a lengthy process for some participants. It is possible that participants did not take their time answering the survey. Furthermore, the results of the survey could be different if this study used the median score instead of the mean score. The survey instrument used in this survey is reliable, but it could benefit from reconstructing the Likert scales. The study calculated the mean of each section of the survey instrument. Though this study has its limitations, the results were similar to the original research by [10].

Recommendations for Further Study

Studies have shown that mobile device security research is a growing field that continues to attract researchers. Although there are various studies on mobile device security, few have considered different forms of IT threats in mobile device security. Therefore, it is essential for researchers to continue to examine changing IT threats concerning mobile device security. Exploring how individuals utilize their mobile device security features will provide insight into security threats. Understanding how mobile device users implement available security software on their mobile devices is an opportunity for further research.

Conclusion

Previous research gaps and limitations identified by previous researchers inspired this study. The study utilized the Technology Threat Avoidance Theory questionnaire [10] to test IT threats and users' behavior. The survey instrument contained 44 Likert-Type scale questions. Survey data collected from 137 mobile device users were tested using the survey instrument. Descriptive statistics, frequencies, Pearson correlation, and regression analysis were used to examine the data collected for statistical analysis. The result of the data analysis rejects the null hypothesis for 1a, 1b, 1c, 2, 3, 3a, 4, 5, and 6, while it supports the alternative hypothesis.

The findings from this study provided information about mobile device users' susceptibility to phishing attacks, mobile device users' security practice behavior, and mobile device users' threat avoidance motivation. The study revealed several findings in the analyses: Avoidance motivation determines avoidance behavior of users, perceived susceptibility and perceived severity positively affect perceived threat, and perceived threat strongly determines avoidance behavior. Thirdly, safeguard effectiveness, safeguard cost, and self-efficacy interact with avoidance behavior. Finally, safeguard cost and perceived threat negatively impact a users' motivation to avoid a threat.

This study examined factors that impact mobile device users' susceptibility to phishing attacks in the United States. The research question for this study was "To what extent, if any, does perceived severity, perceived susceptibility, perceived

threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior influence mobile device users' susceptibility to phishing attacks?" Results from the research indicate a positive correlation between perceived threat, avoidance behavior, and avoidance motivation. The study shows that mobile device users feel threatened if they perceive that the severity of the attack will affect them and, therefore, affects their motivation to avoid phishing attacks threat. Mobile device users in the United States might not take appropriate actions to thwart IT threats, thereby making them susceptible to phishing attacks.

Regarding further research, mobile device security provides new ground for exciting and new research. Further study can improve mobile device users' security behavior, discover new types of security threats, and understand the use of mobile device security software. Researchers could shed more insights on mobile users' security threats by applying valuable techniques. Increased mobile device security awareness can help thwart IT threats; however, users must adopt positive behavior to reduce phishing attack threats.

References

1. Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: an empirical study. Informatics in Education-An International Journal, 15, 235-252. doi:10.15388/infedu.2016.12
2. Hewitt, B., Dolezel, D., & McLeod, A. (2017). Mobile device security: perspectives of future healthcare workers. Perspective in Health Information Management, 1-14.
3. Vishwanath, A. (2016). Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. Computers in Human Behavior, 63, 198-207.
4. Shende, A., & Saveetha, D. (2016). Protection against phishing in mobile phones. International Journal of Computer Science and Information, 14, 228-233.
5. Mouton, F., Malan, M., Kimpaa, K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114-127.
6. Purkait, S. (2012). Phishing counter measures and their effectiveness - literature review. Information Management & Computer Security, 20, 382-420.
7. Liao, Q., & Li, Z. (2014). Portfolio optimization of computer and mobile botnets. Internal Journal Information Security, 13(1), 1-14.
8. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerabilities within an integrated, information processing model. Decision Support Systems, 51, 576-586.
9. Greavu-Serban, V., & Serban, O. (2014). Social engineering a general approach. Informatica Economica, 18(2), 5-14.
10. Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11, 394–413.