ISSN 2712-0562
Original Research

Sustainable Engineering and Innovation
Vol. 6, No. 1, May 2024, pp.87-102
https://doi.org/10.37868/sei.v6i1.id248

Adoption of identity theft protection services in social media: A PMT investigation

Kazi Rubaiyat Shahriar Rahman[1], Omar Faruq[2*], Md. Taufiqur Rahman[3], Md. Rafiujjaman Sumon[4], Md. Atikur Rahman[5], Abu Sazzad Mohammad Parvez[6], Narayan Chandra Nath[7], Tareq Ahmed Sohel[8]

[1] Computer Science and Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
[2] Electrical and Electrical Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
[3,5] Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh
[4] Computer Science and Engineering, Washington University Science and Technology, VA, USA
[6] Electrical, Electrical and Communication Engineering, Military Institute of Science and Technology, Dhaka, Bangladesh
[7] Electrical and Computer Engineering, University of Kassel, Germany
[2,7,8] Information and Communication Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China

*Corresponding author E-mail: OMAR FARUQ, smomarfaruq99@gmail.com

Received Jan.15, 2024
Revised Apr.9, 2024
Accepted Apr.15, 2024

Abstract

In the last few years, social media has become a part of our lives. It is not a website anymore. It offers us blogging, watching videos, and connecting with more people. In our social media profiles, we create our virtual identity. We share every piece of information connected to our lives. Social media has become a very important part of our lives. Social media changes itself tremendously; it also makes it possible for criminals to take their work to another level. Many crimes happen on social media. One of them is identity theft. As we create our own identities on social media. There is a high risk of identity theft. For this reason, many identity theft protection services have been created. With identity theft protection, we are able to protect our identities on social media. Those identity theft production services are my best product because they help us identify identity threats and get rid of them. They give us protection from identity theft in exchange for some monthly fees. But those services are not common in our nation. We don't know if those services will work in our country or not. With this thesis, we will be able to find out the adoption intention of social media identity theft protection services in our country through PMT investigations.

Keywords: Theft protection, Protection motivation theory, Social media, Identity theft, Cybercrime, Internet security

1. Introduction

When an impostor uses a person’s personally identifiable information (PII) as a convenience in addition to scamming society, it's a crime, and it's called identity theft [1, 2]. A person's PII can be acquired in many ways. Including phishing, attacks, safety violations, and stealing. A person's name, social media ID, national ID, banking account number, payment card number, and further private data are subsets of PII. A person's identity can be stored online and offline. When a person puts his personal information in physical form, it will also be considered an offline identity. Such as an identity card form or a bank account form. When a person uses online forms to open any kind of social account, it will be considered an online identity. Identity can be saved both online and offline [3]. Identity theft is increasing every day. Figure 1 shows the number of cases of increasing identity theft. From this study, we can see that identity theft has been increasing rapidly in the last few years. Identity theft happens in many ways such as data breaches, online theft, stolen paper mail, friendly theft while conducting transactions, or lost or stolen wallets. Those are the traditional methods. However, currently, most identity burglaries occur on the Internet. Many types of pop-up ads are shown on many websites, and when a consumer clicks those links, his or her identity has been stolen. Instead of pop-up ads, those links can be sent via email, WhatsApp, or Messenger as a contest or news.

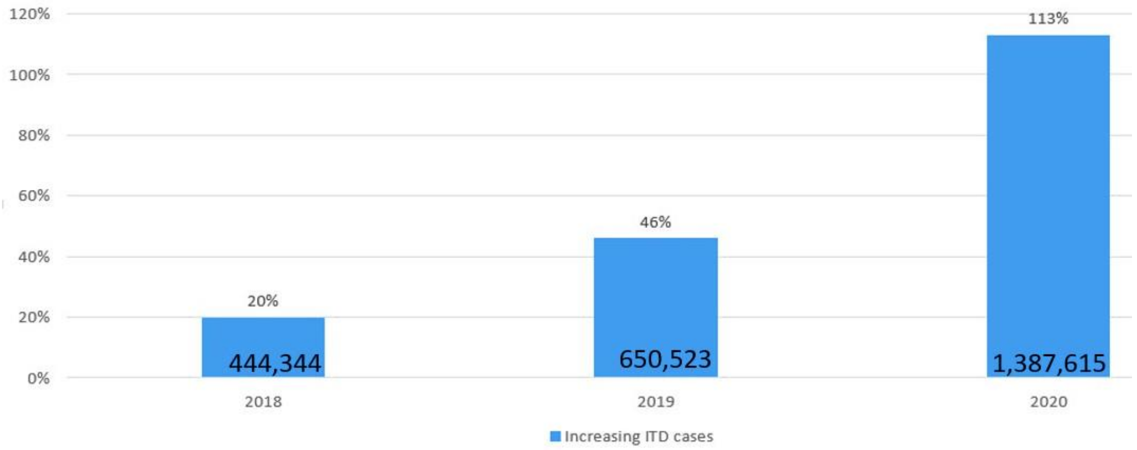

Figure 1. Increasing identity theft (Source: Federal Trade Commission, ftc.gov/data)

When users click the link their identity is stolen. Nowadays, online banking identity theft has become very popular, as have phone calls. In Bangladesh, there is a mobile banking app called Bkash. Bank account holders are called by imposters, and they tell them to tell the OTP. If the consumer doesn't tell the OTP, their account will be banned. So, when a consumer shares the OTP, their identity has been stolen, and that imposter can control his or her account [4].

Social media is a collection of Internet-based applications through which users can generate and exchange information [5]. Social media is a single platform that can attract more people to connect with each other from around the world [6]. In the past, social media websites such as Facebook, Twitter, and Instagram were mainly utilized by youngsters to socialize. But now social media is used by people of all ages. Social media has changed itself so tremendously that now we can learn from it. We can also buy and sell products there. Nowadays, a huge amount of business is done on social media. It has become an important part of our day-to-day lives. Many people have become addicted to social media. Businessmen spend a lot of money advertising their products on social media. This impacted the creation of the social media influencer. People make their identities known on social media. If we see someone's social media account, we will never be able to get to know him without meeting him physically. People who have more followers on social media make a lot of money by advertising as social media influencers.

Social networking offers several benefits. Though the use of social media provides a lot of advantages, it also has a dark side. Many crimes are happening on social media. People are getting harassed, hacked, cloned, and stolen from on social media. Some imposters commit identity theft on social media. Sometimes social media users don't know that their account has been hacked and someone else is also using it. Some criminals use identity theft to commit fraud with others on social media. People store much of their personal information on social media. Identity theft has become a serious issue. Most identity theft happens through social media messages. People get tempting news and lottery results as messages. When users click the link, their identities are stolen.

The most popular social media site is Facebook. Almost every social media user uses Facebook. One-third of social media users give away at least some free data which can lead to identity theft. Success names, date of birth, mobile number, pet names, etc. [7] Facebook completed a survey from the identity theft resource center server named Facebook Social Media Survey. "From the survey, we know ways to prevent identity theft on Facebook. Figure 2 shows the methods for committing identity theft on Facebook [8]. So, we can see some ways that identity theft occurs. In most cases, this is done through private messages from a scam website or through fake links. This happens not just on Facebook but also on Twitter, Instagram, WhatsApp, and many other types of social media are used for identity theft in this way.

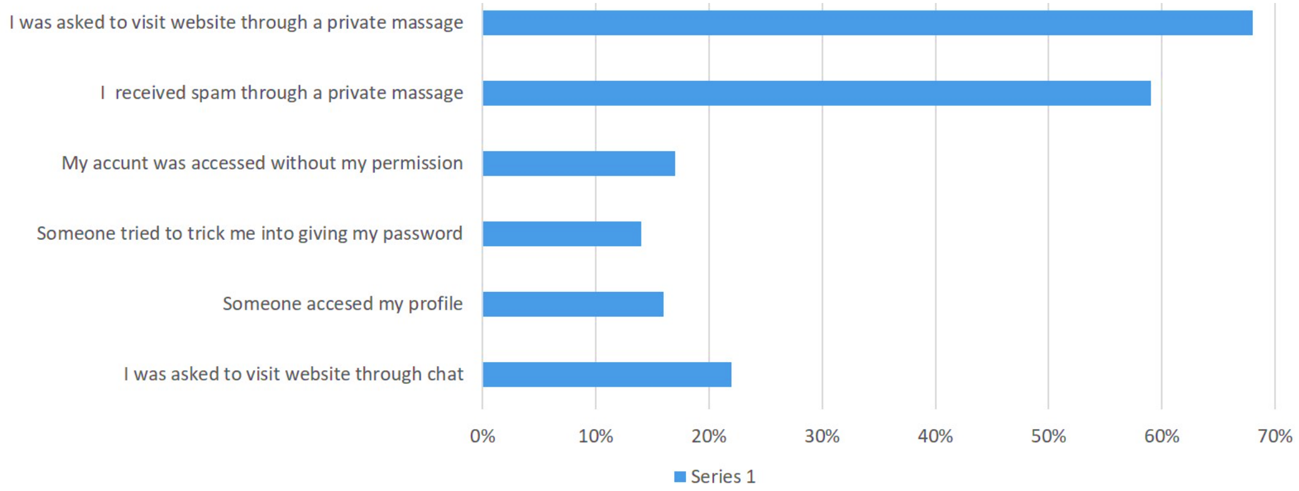

Figure 2. Ten ways to identity theft on Facebook [8]

Social media plays an important role in Bangladesh. Facebook, Twitter, YouTube, etc. are some of the most important social media platforms. When we speak of online platforms, the primary name that immediately comes to mind is Facebook in Bangladesh. The following Figure 3 shows the usage of social media in Bangladesh.

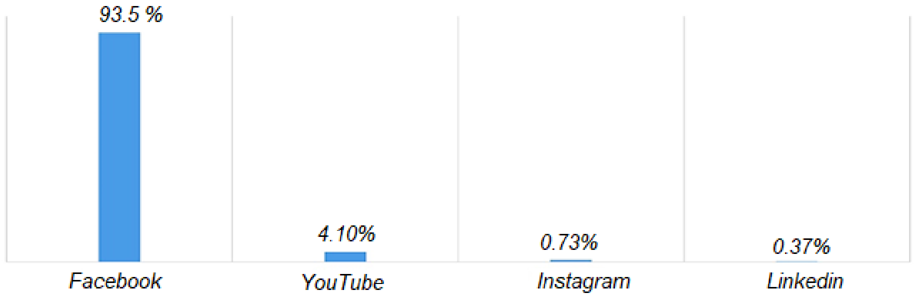

Figure 3. Uses of social media in Bangladesh (2021-2022); source: Statcounter Global Stats

This traffic is for Bangladesh. In the graph, we can see that from March 2021 to March 2022, more than 80% of social media users will use Facebook, Twitter, YouTube, and other social media. In our survey, we saw that most people who live in Dhaka use social media for 2-4 hours a day. Some people use social media for more than four hours a day. So, we can see that social media is very important in Bangladesh. Everything is done on Facebook. People watch many kinds of videos on Facebook. People also update their lifestyles on Facebook in Bangladesh. Recently, Facebook launched Marketplace, with the help of which people can buy and sell anything on Facebook. So, Facebook has become a part of every person in Bangladesh, mainly in Dhaka city.

People are financially and mentally attached to social media in Bangladesh. People create their best versions of themselves on social media. They post every detail. They also shared their private chats on social media. But they don't know they have a huge list of identities. Identity theft can occur on social media very easily. We are vulnerable in terms of how to protect our identity on social media because we do not know how to do so. If someone's identity on social media gets stolen, it will be a huge problem for him. Because someone else will control their identity. His or her privacy can be leaked [9]. He or she can be a financial fraudster. An impostor can lend money to others using his identity. There is also a chance to upload an appropriate thing, such as his ID. Therefore, protecting identity on social media is very important for people living in Bangladesh. That is why we are vulnerable. We can use identity theft protection services to avoid identity theft problems. It will give us confidence to use social media properly because our social media will be safe if we use an identity theft protection service.

Protection motivation theory (PMT) is an approach recommended by everyone as a response to phishing communication, mainly through fear appeals [10]. PMT works to increase consumers' perception of threats and encourage individuals to take the advised steps to minimize their apprehension [11]. PMT is the direct image of the parallel process model [12]. Identity theft is covered under Internet security. Many researchers have investigated Internet security due to PMT investigations in the past [13].

Table 1. Works of is in PMT

Authors	Title	Domain	Theory
[14]	When anybody is looking, I'll carry out what you're about to want to know: Mandatory, Management, and Safety of Information	Information Security	PMT
[15]	The impact of fear as well as information protection behaviors: a laboratory investigation	Information Security	PMT
[16]	The reasons for wanting Information Security: The theory of protective motivation vs. the Hypothesis of Self-Determination	Information Security	PMT
[16]	A multifaceted investigation of the effect of collective and social ownership on protective behavior.	Information Security	PMT

From Table 1, we can understand that protection motivation theory is best for Internet security research. We are researching the adoption of identity theft prevention services. We can utilize PMT in this research.

There are two objectives for clarifying this study:

1. Test the impact of PMT on adoption and wishful thinking, such as determining the influence of PMT factors on the desire to use identity theft protection services for their customers.

2. Test the impact of PMT variables on wishful thinking.

2. Background studies

2.1. Protection motivation theory (PMT)

PMT is a theory that recommends that everyone may respond to an attack in communication, mainly through fear appeals [17]. PMT works to increase consumers' perception of dangers and encourage people to undertake the advised steps to minimize the anxiety they feel [18]. Although PMT was established in the field of health to consider ethnic background, cigarette smoking, and other disorders [19], investigators discovered it valuable in the field of cybersecurity. The primary PMT by Rogers addresses the different elements of fair arguments and how coping and taking a protective behavior response are influenced by the door components. But then, in 1983 [20], self-efficiency and the cost associated with protective behavior were added to PMT. Figure 4 depicts the protection motivation theory (1983) [21].

The perception of vulnerability along with seriousness is included in threat appraisal, as can be believed advantages linked to a dangerous attitude. Extreme susceptibility and severity predispose individuals to higher protection motivation. In self-sufficiency, individuals believe that they should hold onto their own individual capacity to undertake safeguarding conduct and, in turn, be knowledgeable concerning how effective it is to protect oneself [22]. Response costs are costs associated with protective behavior.

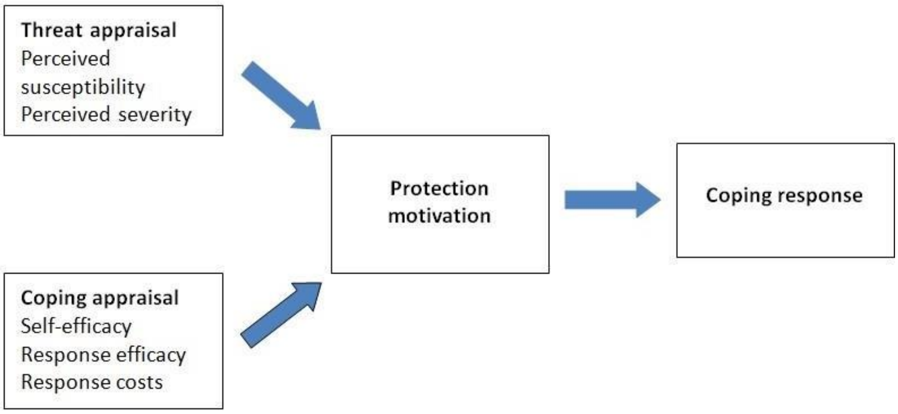

Figure 4. Protection motivation theory (1983)

2.2. Previous works

Identity theft protection falls under the information security domain. There is much previous work in information security that has been completed with protection motivation theory. For example, those are some research papers in protection motivation theory, shown in Table 2.

Table 2. Previous works on PMT

Sl.	References	Year	Journal / Conference name	Country	Sample type	Sample size	Number of citations	Application	Variance
1	[11]	2017	Journal of Computer and Security	Australia	Home computer and mobile device users	629	105	Information security	77.61%
2	[22]	2019	International Journal of Bank Marketing	Taiwan	Debit or credit card users	418	6	Information security	70%-92%
3	[23]	2013	Journal of Information Privacy and Security	England	IT students	77	41	Information security	67%
4	[24]	2013	Computers in Human Behavior	USA	Online market-research firm	741	68	Information security	39%
5	[25]	2021	The DATA BASE for Advances in Information Systems	Nürnberg	Form research papers	-	1	Information security	33%-44%
6	[26]	2020	International Journal of Cancer Management	Iran	Women	410	6	health	25%
7	[27]	2020	Health information on social media	China	Chinese older adult users of WeChat	290	15	Information security	46%-55%

Sl.	References	Year	Journal / Conference name	Country	Sample type	Sample size	Number of citations	Application	Variance
8	[18]	2018	International Journal of Human-Computer Studies	Spain	Sample of Internet users	2024	101	Information security	66%-73%
9	[28]	2020	Dove Press journal	Australia	Older people of 60–88 years,	300	13	Information security	27%
10	[29]	2015	Information Systems Management	USA	Undergraduate students	241	173	Information security	46%

2.3. Wishful thinking

Wishful thinking is part of the protection and motivation theory. At PMT, we talk about fair appeal. If we have fairness for identity theft, we also wish that identity theft wouldn't happen and that identity problems would be solved without doing anything. In our survey, one of our objectives is to test the impact of empty variables on wishful thinking. We will be testing PMT factors such as apparent danger, degree of severity, susceptibility, reaction cost, effectiveness, and independence influence on wishful thinking [30, 31] as we are working on identity theft on social media. There are a few wishful thoughts; identity theft on social media will go away, somehow you will come across a magical solution, suddenly identity theft on social media will disappear by itself, etc.

2.4. Research gap

Our research purpose is to experiment with the impact of PMT variables on wishful thinking and the desire to provide safeguarding from identity theft services to their customers [32]. This research is taking place in Bangladesh, specifically in Dhaka. The data we collect is from social media users in Dhaka. Our results will not be for the whole country [33]. So, this is the first research gap. Another thing is that identity theft protection services have not been quite popular in Bangladesh till now. Therefore, the people of Dhaka know little about identity theft criteria. This is another research gap in this research. But soon, this research will help when identity theft happens on a large scale. People are expected to adopt identity theft protection services [34, 35].

3. Research methodology

3.1. Research model

The study approach involves focusing on PMT characteristics, which include expected danger intensity, risk, reaction performance, expense, and perceived self-efficiency (Figure 5). We can see that we are testing PMT factors on wishful thinking as well as would like to use fraudulent activity prevention resources on social networking sites through this research model. In this model, we can see that every PMT variable has a positive or negative impact on the thinking of society and the intention to adopt. So, we call those H1, H2, and H10. We found a total of 10 hypotheses. We will test 10 hypotheses from our data.

3.2. Perceived severity

Perceived severity stands for the seriousness of the potential danger of getting your identity stolen on networking sites. We assume that, at present or in the future, social media identity theft will be a serious problem. So, we have a hypothesis that the level of severity provides a beneficial impact overall on the utilization of identification prevention services and a detrimental impact on unrealistic expectations. We have two hypotheses:

[H1] The degree of severity perceived has a beneficial influence on the propensity to use identity theft protection services.

[H6] The reported harshness implies a detrimental influence on wishful thinking.

3.3. Perceived vulnerability

Perceived vulnerability stands for how vulnerable we are to protecting our identity on social media.

It has a strong impact on the reported harshness, which implies a detrimental influence on wishful thinking. We have two hypotheses.

[H2] The feeling of weakness provides a beneficial influence on the plan to switch identity theft protection services.

[H7] Wishful thinking is influenced negatively by perceived weakness.

3.4. Perceived responsive efficacy

This concept pertains to an individual’s expectations about their behavior regarding identity theft. It has an impact on adapting IDT protection services. We have two hypotheses.

[H3] Perceived response: the effectiveness has a good impact on the desire to become a parent identity theft protection service.

[H8] Perceived responding to the effectiveness exerts an undesirable consequence on wishful thinking.

3.5. Response cost

Response costs are tense for individuals' willingness to adopt identity theft protection services, with their service charges having an impact on wishful thinking. People might think of wishful thinking as a response cost. We must hypothesize.

[H4] Perceived response costs have a negative impact on the aim of embracing fraud security solutions.

[H9] Perceived response costs have a favorable influence on optimistic thinking.

3.6. Perceived self-efficacy

Self-efficiency stands for an individual’s willingness to adopt identity theft protection on social media. It has an impact on PMT variables.

[H5] The overall perceived sense of self-worth has pushed a beneficial influence on the desire to change identity theft protection services.

[H10] Perceived self-efficacy has a negative influence on optimistic thinking.

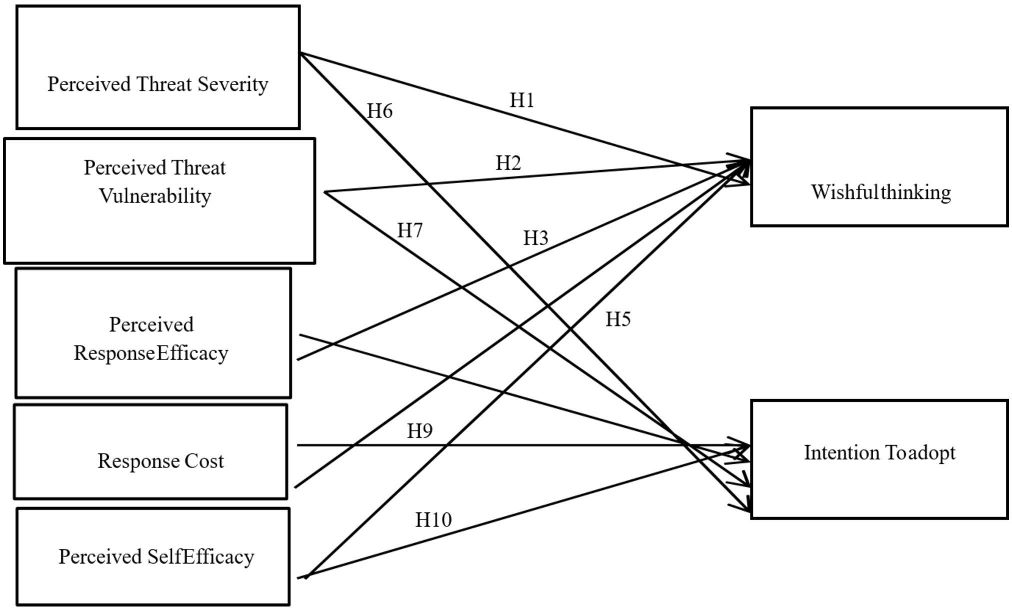

Figure 5. Research model

4. Result and analysis

4.1. Sample and data collection

We used a service-based approach using an online Google form with questionnaires, and we got our data to test our hypothesis. Our form is for people who live in Dhaka, are older than 15 years old, and use social media, as shown in Table 3.

Table 3. Measurement item

Variable	No.	Measurement Items	Source
Perceived severity	PS1	An identity theft on social media could represent a significant issue on my behalf as well.	[11]
	PS2	Loss of identity consequences would have been significant for anyone.	
	PS3	Possessing work or identity on social media sites exposed to anyone without my consent or understanding may be a big concern for me.	
	PS4	A significant assault, including harm to my personal social media persona, might look quite bad for me.	
	PS5	I think identity theft on social media is harmful.	
	PS6	I believe that protecting your identity on social media is important.	
Perceived vulnerability	PV1	My social media accounts could be subject to serious identity theft if I fail to follow identity theft protection services.	[11]
	PV2	My social media will face more and more identity thefts if I fail to follow identity theft protection services.	
	PV3	My social media accounts will face more and more identity theft if I fail to follow identity theft protection services.	
	PV4	My social media accounts could be at risk of identity theft if I fail to follow identity theft protection services.	
	PV5	My social media accounts will suffer from identity theft if I fail to follow identity theft protection services in the future.	
	PV6	My social media accounts will be at risk of identity theft if I fail to follow identity theft protection services.	
Perceived self-efficacy	PSE1	My social media accounts could fall victim to identity theft if I fail to follow identity theft protection services.	[11]
	PSE2	I'm confident in implementing actions to protect myself and my social media using identity theft protection services.	
	PSE3	Taking the necessary security measures using identity theft protection services is entirely under my control.	
	PSE4	I am equipped with the means as well as expertise for performing the essential security precautions utilizing identity theft protection services.	
	PSE5	Taking the necessary security measures is easy with identity theft protection services.	
	PSE6	I can protect my social media by myself using identity theft protection services.	
Perceived response	PRE1	I can enable security measures using identity theft protection services on my social media.	[11]
	PRE2	Enabling security measures using identity theft protection services on my social media will prevent identity theft.	
	PRE3	Implementing security measures using identity theft protection services on social media is an efficient method of preventing identity theft.	

Variable	No.	Measurement Items	Source
	PRE4	Enabling safety safeguards and utilizing identity theft protection services on my social media will prevent identity theft.	
Response cost	RC1	Preventive actions exist to prohibit someone from obtaining private information relating to one's finances or personal life through identity theft protection services on social media.	[11]
	RC2	Implementing safety regulations for identity theft protection services on social media is problematic for me.	
	RC3	We have sufficient additional expenditures involved with utilizing identity theft protection services to protect my social media.	
	RC4	Implementing safety regulations for identity theft protection services on social media would require considerable investment and effort.	
	RC5	Implementing safety regulations for identity theft protection services on social media would be time-consuming.	
	RC6	The price tag of adopting appropriate procedures for safety with identity theft protection services on social media is as high as the advantages.	
Adoption intention	AI1	It turns out that the security safeguards of utilizing identity theft protection services on social media are as numerous as the advantages.	[27]
	AI2	I am willing to adopt identity theft protection services for social media security purposes.	
	AI3	I intend to adopt identity theft protection services for social media safety purposes in the future.	
	AI4	I guess I will consistently attempt to become an adoptive of identity theft protection services for social media safety purposes in the future.	
Wishful thinking	WT1	I guess I will consistently attempt to become an adoptive family of protection services for social media safety purposes in the future.	[36]
	WT2	My social media accounts will face more and more identity theft if I fail to follow identity theft protection services.	
	WT3	My social media accounts could be at risk of identity theft if I fail to follow identity theft protection services.	
	WT4	My social media accounts will suffer from identity theft if I fail to follow identity theft protection services in the future.	

4.2. Measurement model

We have developed our questionnaires based on PMT variables. Our survey form has three sections. In the first section, we asked people about their place of residence and use of social media. In the second section, we ask many questions about PMT variables. In the third section, users' details were asked. We took the respondents' opinions on a 7-point scale, ranging from 1 (strongly disagree) to 7 (strongly agree).

4.3. Analysis of the measurement model

Validly collected data has been analyzed using PLS 3.0 software. We extracted our data from the Google form into an Excel sheet. Then we upload our Excel sheet to PLS 3.O. We developed our own research model. We get composite reliability, average variance extracted, and correlation between constructs from PLS. Based on the correlation matrix, discriminatory validity was tested. From Fornell and Larcker [13], we know that to assure discriminatory validity, two conditions must be fulfilled: (a) all AVE should be greater than 0.50; (b) the square root of AVE is data greater than all cross-correlation. In Table 4, we saw that AVE's range is from 0.59 to 0.86, and all square roots of AVE are greater than all cross-correlations [37, 38]. So, we can say that our result is assured for our study.

Table 4. Composite, reliability, average variance extracted (AVE), loading factors

	Composite reliability	Average variance extracted (AVE)	AI	PRE	PS	PSE	PV	RC	WT
AI	0.940	0.797	0.893						
PRE	0.895	0.682	0.532	0.826					
PS	0.897	0.594	0.362	0.441	0.771				
PSE	0.950	0.761	0.550	0.592	0.404	0.872			
PV	0.921	0.659	0.596	0.549	0.530	0.516	0.812		
RC	0.975	0.869	-0.295	-0.150	-0.109	-0.242	-0.149	0.932	
WT	0.957	0.848	-0.303	-0.090	-0.105	-0.211	-0.208	0.571	0.921

4.4. Analysis of the structural model

We have created our structural model in PLS 3.0, and we get our result from the structural model. Figure 6 shows the result of the research model. The result of the analysis of the model is shown in Table 5.

Table 5. Variance

Sl.	Objective	Result (*R*2)	%
1	Impact of PMT variables on the intention to adopt identity theft protection services.	0.478	47%
2	Impact of PMT variables on wishful thinking.	0.350	35%

This is a structural model with results. We got the result from SmartPLS 3.0. In security studies, the set of original PMT constructs generally accounts for 0.34-0.50 of the variance [39]. We got the variance (R2) from the analysis by test of our hypothesis, shown in Figure 6. Hypothesis testing parameters are shown in Table 6.

Table 6. Hypothesis testing

Hypothesis	Hypothesis path between	Path coefficients	t-values	Supported?
H1	Perceived severity → adopt identity (+)	-0.020	0.185	no
H2	Perceived vulnerability → adopt identity (+)	0.368	2.956	yes
H3	Perceived response efficacy → adopt identity (+)	0.183	1.639	yes
H4	Perceived response cost → adopt identity (-)	-0.161	2.071	yes
H5	Perceived self-efficacy → adopt identity (+)	0.222	2.087	yes
H6	Perceived severity → wishful thinking (-)	0.019	0.170	no
H7	Perceived vulnerability → wishful thinking (-)	-0.164	1.528	yes
H8	Perceived response efficacy → wishful thinking (-)	0.115	1.037	no
H9	Perceived response cost→ wishful thinking (+)	0.549	6.618	yes
H10	Perceived self-efficacy→ wishful thinking (-)	-0.069	0.492	yes

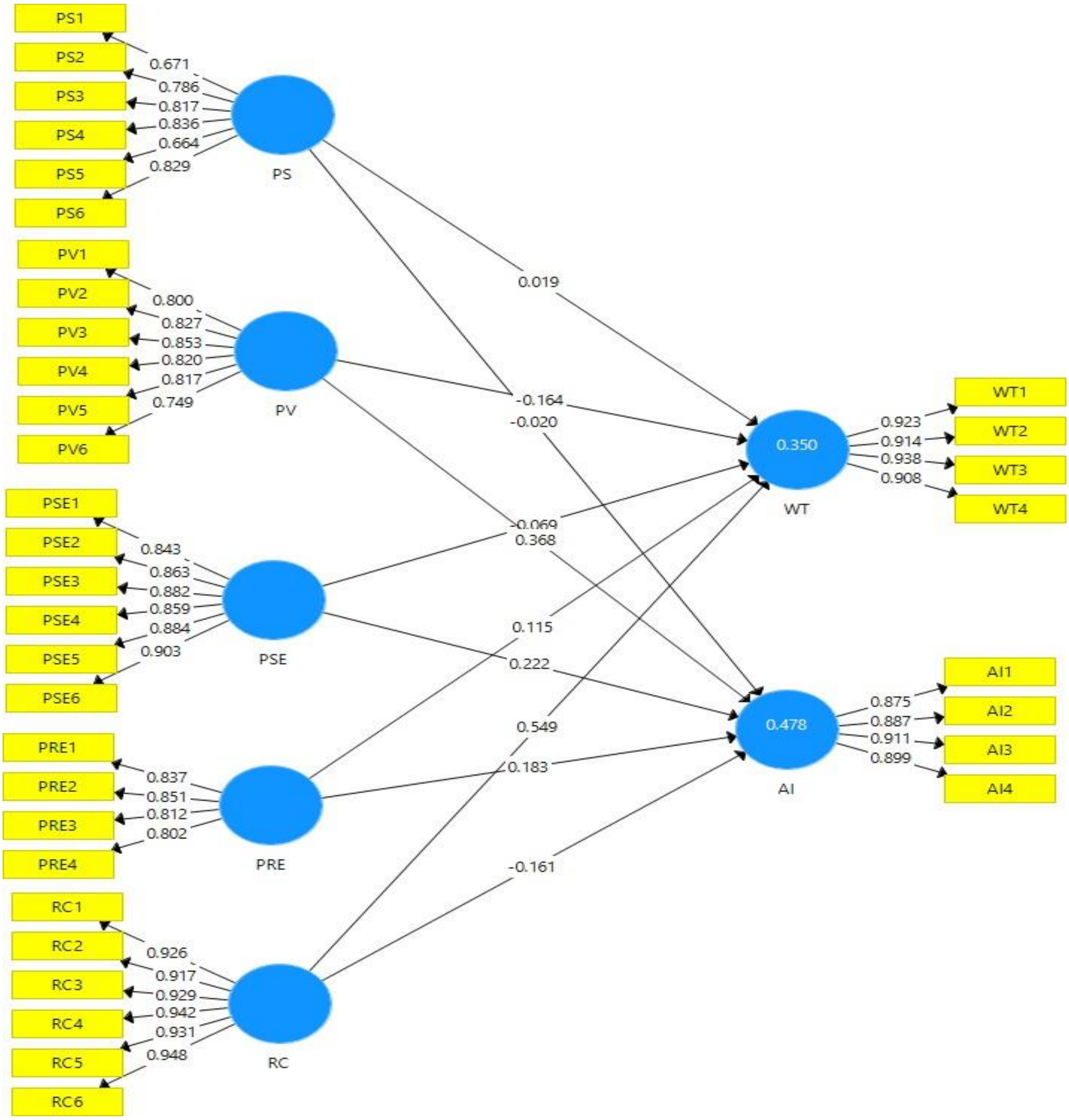

Figure 6. Result of the research model

5. Result and discussion

5.1. Discussion of results

Read the PMT, where you should always experiment with the impact of PMT variables on adoption intention and wishful thinking. Our objective was to analyze the effect of PMT variables on the adoption of identity theft production services via social networking sites, along with the consequences of PMT factors affecting wishful thinking. In Table 5, we can see that the impact of PMT variables on adopting identity theft protection services is 47%, and the impact of PMT variables on wishful thinking is 35%. So, adoption intention is greater than wishful thinking. So, from our research, we can understand that most people don't want wishful thinking and think IDT is a problem. They have a high risk of identity theft. So, most of them want to adopt identity theft protection services. On the other hand, when we talk about PMT, we always come up with hypotheses. So, there were 10 hypotheses in our study. Seven hypotheses were supported by the respondents. But only the third hypothesis doesn't support it. Hypothesis: perceived severity has a positive impact on adopted identity. But as a result, we can see that the path coefficient is -0.02, which is negative. It has a little negative value, so we can say that there is a weak effect. In the same way, perceived severity has a positive effect on wishful thinking. So as per our study, we can say that if we want to work with an identity theft protection service, we must take care of those three loading factors.

5.2. Theoretical and practical contribution

Every research project has its own theoretical and practical sites. From PMT, we get a theoretical hypothesis. We have 10 hypotheses in our research. In theory, we believe that the lost hypothesis will support our research model. But when we started taking data from Facebook users, we saw that not all hypotheses were supported. After completing our data collection, when we analyzed the data, we saw that seven hypotheses were supported and one was not. So, this is the practical side of our research paper.

5.3. Future works

Though we have some limitations in our research, there are some future projects in this study. We only take data from Dhaka. In the future, we can get data from all over Bangladesh and do this type of research. We know PMT is quite popular with information security-based researchers. But in the case of identity theft protection service adoption, PMT is new, and we can improve our PMT model in the future. Our other limitation is that lots of people don't know about identity theft and identity theft protection services. So, when identity theft becomes a problem in the future, this recharge can be upgraded. Today, social media has become very important in our lives. But most people have no economic attachment to social media. In China, there is a social media site called WeChat. Chinese citizens can make any kind of economic payment with their social media. Soon, social media will be everything for people. In that time, identity theft can become a huge problem for society, and identity theft protection services will be adopted by everyone, so there are many chances for future work on this topic.

6. Conclusion

In conclusion, we can say that identity protection services on social media should be used by everyone since social media has become so integral in society. These days, a huge number of people are creating content on social media and earning a huge amount of money. So, there is a high risk of identity theft through social media, which is increasing day by day. The identity theft protection problem is not an easy one to solve by itself. We must adopt identity theft protection services to protect ourselves. However, identity theft protection services need to be affordable and available for all. Therefore, in our research, we understand that people will adopt identity theft protection services to get rid of the problem. Another thing we saw was that when response costs are lower, people are more attracted to taking protection against identity theft.

Declaration of competing interest

We declare that have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: K.R.S. Rahman, O. Faruq: study conception and design; M. T. Rahman, M. A. Sumon, M. A. Rahman, T. A. Sohel: data collection; A. S. M. Parvez, N. C. Nath, K.R.S. Rahman, O. Faruq: analysis and interpretation of results; O. Faruq: draft preparation. All authors approved the final version of the manuscript.

Ethical approval statement

Ethical approval is not applicable for this research.

References

[1] S. Irshad and T. R. Soomro, "Identity Theft and Social Media"," IJCSNS International Journal of Computer Science and Network Security, vol. 18, no. 1, pp, 43-55, 2018. http://search.ijcsns.org/07_book/html/201801/201801006.html, http://paper.ijcsns.org/07_book/201801/20180106.pdf

[2] I. Bose, Indian Institute of Management Calcutta, A. C. Man Leung, and City University of Hong Kong, "Adoption of identity theft countermeasures and its short- and long-term impact on firm value," MIS Q, vol. 43, no. 1, pp. 313–327, 2019. https://doi.org/10.25300/misq/2019/14192

[3] F. Lai, D. Li, and C.-T. Hsieh, "Fighting identity theft: The coping perspective," Decis. Support Syst., vol. 52, no. 2, pp. 353–363, 2012. https://doi.org/10.1016/j.dss.2011.09.002

[4] O. Ogbanufe and R. Pavur, "Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection," Int. J. Inf. Manage., vol. 62, no. 102432, p. 102432, 2022. https://doi.org/10.1016/j.ijinfomgt.2021.102432

[5] J. van Dijck, The culture of connectivity: A critical history of social media. Oxford University Press, 2013. 10.1093/acprof:oso/9780199970773.001.0001

[6] H. M. Salman, "Identity theft on social media for the system of banking sector in Islamabad," SSRN Electron. J., 2020. https://doi.org/10.2139/ssrn.3679244

[7] R. W. Rogers, "A protection motivation theory of fear appeals and attitude Change1," J. Psychol., vol. 91, no. 1, pp. 93–114, 1975. https://doi.org/10.1080/00223980.1975.9915803

[8] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," Commun. Monogr., vol. 59, no. 4, pp. 329–349, 1992. https://doi.org/10.1080/03637759209376276

[9] K. Marett, Mississippi State University, A. McNab, R. Harris, Niagara University, and Indiana University, "Social networking websites and posting personal information: An evaluation of protection motivation theory," AIS Trans. Hum.-Comput. Interact., vol. 3, no. 3, pp. 170–188, 2011. https://doi.org/10.17705/1thci.00032

[10] H. Leventhal, "Findings and theory in the study of fear communications," in Advances in Experimental Social Psychology, Elsevier, 1970, pp. 119–186. https://doi.org/10.1016/s0065-2601(08)60091-x

[11] N. Thompson, T. J. McGill, and X. Wang, "'Security begins at home': Determinants of home computer and mobile device security behavior," Comput. Secur., vol. 70, pp. 376–391, 2017. https://doi.org/10.1016/j.cose.2017.07.003

[12] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," J. Exp. Soc. Psychol., vol. 19, no. 5, pp. 469–479, 1983. https://doi.org/10.1016/0022-1031(83)90023-9

[13] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," J. Mark. Res., vol. 18, no. 1, pp. 39–50, 1981. https://doi.org/10.1177/002224378101800104

[14] S. H. Kim, K. H. Yang, and S. Park, "An integrative behavioral model of information security policy compliance," ScientificWorldJournal, vol. 2014, pp. 1–12, 2014. https://doi.org/10.1155/2014/463870

[15] A. T. Shappie, C. A. Dawson, and S. M. Debb, “Personality as a predictor of cybersecurity behavior,” Psychology of Popular Media, vol. 9, no. 4, pp. 475–480, 2020. https://psycnet.apa.org/doi/10.1037/ppm0000247

[16] P. Menard, G. J. Bott, and R. E. Crossler, “User motivations in protecting information security: Protection motivation theory versus self-determination theory,” J. Manag. Inf. Syst., vol. 34, no. 4, pp. 1203–1230, 2017. https://doi.org/10.1080/07421222.2017.1394083

[17] T. Sommestad, H. Karlzén, and J. Hallberg, “A meta-analysis of studies on protection motivation theory and information security behaviour,” Int. J. Inf. Secur. Priv., vol. 9, no. 1, pp. 26–46, 2015. https://doi.org/10.4018/ijisp.2015010102

[18] R. van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, “Using protection motivation theory in the design of nudges to improve online security behavior,” Int. J. Hum. Comput. Stud., vol. 123, pp. 29–39, 2019. https://doi.org/10.1016/j.ijhcs.2018.11.003

[19] R. Shillair, “Protection Motivation Theory,” The International Encyclopedia of Media Psychology. Wiley, pp. 1–3, 09-Sep-2020. https://doi.org/10.1002/9781119011071.iemp0188

[20] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, “Exploring motivations for online privacy protection behavior: Insights from panel data,” Communic. Res., vol. 48, no. 7, pp. 953–977, 2021. https://doi.org/10.1177/0093650218800915

[21] I. Tahir, B. Budiono, A. Armansyah, and A. Hendri, “Histonomic approach: Did FDI affect labor productivity in Indonesia after economy crisis in 1998?,” in Proceedings of the International Conference on Economic, Management, Business and Accounting, ICEMBA 2022, 17 December 2022, Tanjungpinang, Riau Islands, Indonesia, 2023. http://dx.doi.org/10.4108/eai.17-12-2022.2333262

[22] S.-T. Wang, “The effects of risk appraisal and coping appraisal on the adoption intention of m-payment,” Int. J. Bank Mark., vol. 38, no. 1, pp. 21–33, 2019. https://doi.org/10.1108/IJBM-10-2018-0272

[23] P. Meso, Y. Ding, and S. Xu, “Applying protection motivation theory to information security training for college students,” J. Inf. Priv. Secur., vol. 9, no. 1, pp. 47–67, 2013. https://doi.org/10.1080/15536548.2013.10845672

[24] T.-M. (catherine) Jai, L. D. Burns, and N. J. King, “The effect of behavioral tracking practices on consumers’ shopping evaluations and repurchase intention toward trusted online retailers,” Comput. Human Behav., vol. 29, no. 3, pp. 901–909, 2013. https://doi.org/10.1016/j.chb.2012.12.021

[25] S. Haag, M. Siponen, and F. Liu, “Protection motivation theory in information systems security research: A review of the past and a road map for the future,” SIGMIS Database, vol. 52, no. 2, pp. 25–67, 2021. https://doi.org/10.1145/3462766.3462770

[26] F. Ghofranipour, F. Pourhaji, M. H. Delshad, and F. Pourhaji, “Determinants of breast cancer screening: Application of protection motivation theory,” Int. J. Cancer Manag., vol. 13, no. 5, 2020. https://doi.org/10.5812/ijcm.100535

[27] L. Shang, J. Zhou, and M. Zuo, “Understanding older adults’ intention to share health information on social media: the role of health belief and information processing,” Internet Res., vol. 31, no. 1, pp. 100–122, 2020. https://doi.org/10.1108/INTR-12-2019-0512

[28] Z. Taheri-Kharameh, S. Bashirian, R. Heidarimoghadam, J. Poorolajal, M. Barati, and É. Rásky, “Predictors of fall protective behaviors among Iranian community-dwelling older adults: An application of the protection motivation theory,” Clin. Interv. Aging, vol. 15, pp. 123–129, 2020. https://doi.org/10.2147/CIA.S224224

[29] M. D. Hanus and J. Fox, “Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance,” Comput. Educ., vol. 80, pp. 152–161, 2015. https://doi.org/10.1016/j.compedu.2014.08.019

[30] M. R. Ab Hamid, W. Sami, and M. H. Mohmad Sidek, “Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion,” J. Phys. Conf. Ser., vol. 890, p. 012163, 2017. https://doi.org/10.1088/1742-6596/890/1/012163

[31] R. Ezati Rad et al., “Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study,” BMC Public Health, vol. 21, no. 1, 2021. https://doi.org/10.1186/s12889-021-10500-w

[32] M. J. Zare Sakhvidi, M. Zare, M. Mostaghaci, A. H. Mehrparvar, M. A. Morowatisharifabad, and E. Naghshineh, “Psychosocial predictors for cancer prevention behaviors in workplace using protection motivation theory,” Adv. Prev. Med., vol. 2015, pp. 1–9, 2015. https://doi.org/10.1155/2015/467498

[33] H. Mehraj et al., “Protection motivation theory using multi-factor authentication for providing security over social networking sites,” Pattern Recognit. Lett., vol. 152, pp. 218–224, 2021. https://doi.org/10.1016/j.patrec.2021.10.002

[34] D. Zhang, F. Su, X. Meng, and Z. Zhang, “Impact of media trust and personal epidemic experience on epidemic prevention behaviors in the context of COVID-19: A cross-sectional study based on protection motivation theory,” Front. Public Health, vol. 11, 2023. https://doi.org/10.3389/fpubh.2023.1137692

[35] M. Cismaru and A. M. Lavack, “Marketing communications and protection motivation theory: Examining consumer decision-making,” Int. Rev. Public Nonprofit Mark., vol. 3, no. 2, pp. 9–24, 2006. https://doi.org/10.1007/bf02893617

[36] D. Q. Chen and H. Liang, “Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory,” IEEE Trans. Eng. Manage., vol. 66, no. 4, pp. 552–567, 2019. http://dx.doi.org/10.1109/TEM.2018.2835461

[37] A. Skalkos, A. Tsohou, M. Karyda, and S. Kokolakis, “Exploring users’ attitude towards privacy-preserving search engines: a protection motivation theory approach,” Inf. Comput. Secur., 2023. https://doi.org/10.1108/ics-08-2022-0142

[38] D. Tsoy, D. Godinic, Q. Tong, B. Obrenovic, A. Khudaykulov, and K. Kurpayanidi, “Impact of social media, Extended Parallel Process Model (EPPM) on the intention to stay at home during the COVID-19 pandemic,” Sustainability, vol. 14, no. 12, p. 7192, 2022. https://doi.org/10.3390/su14127192

[39] M. Sedek, R. Ahmad, and N. F. Othman, “Motivational factors in privacy protection behaviour model for social networking,” MATEC Web Conf., vol. 150, p. 05014, 2018. https://doi.org/10.1051/matecconf/201815005014.