Indian Journal of Economics & Business, Vol. 20, No.1 (2021) : 195-204

EVALUATION OF INTERNET TRANSACTION FRAUD IN THAILAND

TANPAT KRAIWANIT[1] AND PIROONRAT SRIJAEM[2]

Abstract: *This research examines the factors influencing internet transaction fraud in the digital era in Thailand. The population of this study consists of Thai internet users, and the samples were selected using convenience sampling. The statistical method used to test the hypothesis is analysis of covariance (ANCOVA).Internet transaction fraud in this study is evaluated as the total value of damage caused by internet scams, which is a dependent variable.The findings show that age, income and social media plat forms influence the total value of damage significantly.In this examination, the value of economic damage caused by internet transaction fraud equals 214,488.2 million baht or US$7,149.605 million. It is recommended that public sectors create policies to prevent internet fraud, such as spreading useful information about internet scams. Additionally, Internet users should be careful about revealing personal information via online platforms and double-check all the information before confirming a transaction. Finally, providers and online platform owners should improve cyber security systems by updating to the most recent security software.*

Keywords: *Financial transaction fraud, internet transactions, internet fraud, smart phone users*

Received: 28th February 2021 ***Revised: 05th April 2021*** ***Accepted: 24th April 2021***

INTRODUCTION

The role of technology has increased rapidly, and technology is not limited to business sectors but also widely influences people's daily lives. Since smart phones have recently been developed to foster better mobile internet operations, the growth rate of financial transactions conducted via online platforms is increasing. Customers' behaviour has changed; therefore, the ease of internet banking services fulfils users' needs, such as time and cost savings (Wang, Xiang and Fesenmaier, 2014). Another trend is the rapid increase in e-commerce and m-commerce due to the growth in popularity of online shopping, with people usually opting for mobile banking as an online channel for their payments. Thus, the rate of mobile banking use is increasing steadily (Shaikh and Karjaluoto, 2015). In Thailand, cashless payment systems, such as e-wallet and QR code payments, are available in some shops and for some services, particularly among financial institutions that are aware of technological developments and adjust their payment systems to be compatible with this new technology. As a result, Thailand will become a cashless

1 Rangsit University, Thailand, Faculty of Economics, Rangsit University, Pathum Thani 12000, Thailand, Email: tanpat.k@rsu.ac.th

2 Rangsit University, Thailand, Faculty of Economics, Rangsit University, Pathum Thani 12000, Thailand, Email: pangzaa_1990@hotmail.com

society in the next few years (Songwanich, 2016).

As a variety of devices that can connect to the Internet have been launched in markets globally, the prices of these devices have tended to decrease, and therefore customers have more options (OECD, 2014). The consistent growth in online payments via such devices, together with their developing efficiency, leads to new payment methods that will have a significant role in future payment systems. The key factors affecting the acceptance of online payment services are the reliability, stability and security of the system for the customers, excellent customer service, ease of use and the satisfaction of customers' expectations (Chogo and Sedoyeka, 2014). The study by Ozturk, Bilgihan, Salehi-Esfahani and Nan Hua (2017) indicates that, even though mobile banking provides convenience and ease, some users are still concerned about the security systems of mobile banking applications.

Technological developments have changed people's lifestyles, business patterns and the global economy dramatically – especially modern disruptive technologies that alter human lifestyle patterns, for example the Internet of Things (IOT), which provides ease and convenience for daily life and the new online lifestyle (Emmanuel, 2015). In spite of the many advantages of these cutting-edge technologies, there are numerous dangers caused by fraudsters who use online channels to deprive victims of essential personal information to gain benefits and hence harm victims through fraudulent activities (Association of Certified Fraud Examiners, 2019). Fraudsters might create a seminar at a luxury hotel or elegant office building, with an honourable-looking speaker who is able to persuade many people to participate in crypto currency fundraising. However, in the end, the fraudsters cheat their investors. Swindlers sometimes use the same method as a Ponzi scheme, telling investors that they will earn high returns if they can convince many others to invest in crypto currency. The victims might receive high returns in the first month, but afterwards they will not earn any returns (Corbet, Cumming, Lucey, Peat and Vignec, 2019).

In 2019, there were 57 million internet users among the total Thai population of 69.11 million people, equivalent to 82.48%. Social media users accounted for 51 million users; among these users, 46 million accessed social media via smart devices.The number of mobile phone numbers registered in Thailand, amounting to 93.61 million numbers, is greater than the number of Thai citizens (WP, 2018).

Therefore, it is interesting to study internet transaction fraud in the digital era to set guidelines for related regulations. The findings in this study could be applied in the field of financial technology and innovation development, such as functions, security systems, risks of cybercrime and operating systems, and, as a result, reliability in security will be established and customers' expectations will be met.

OBJECTIVES

1. To study the factors that lead to internet transaction fraud in the digital era.

2. To study the factors involved in the perception of information via online networks' effects on internet transaction fraud in the digital era.

DEFINITION OF INTERNET TRANSACTION FRAUD

The Northern Territory Government of Australia defines the most common types of internet transaction fraud as the following (Northern Territory Government of Australia, 2015):

1. Text message scam (smashing) – The victims receive an SMS or MMS that tricks them into subscribing, following or clicking on a link, and then the scammer sends bills asking the victims to pay for services.
2. Online shopping scam – This fraud covers all online transactions, such as goods and service sales, payments and online ads. Scammers offer excellent goods or services at incredibly low prices. If the victims purchase these items, they will never receive the products at all or fake products will be sent instead.
3. Credit card fraud – The victims' credit cards are stolen, and fraudsters use these stolen cards to purchase online goods and services. However, the credit card owners can sue for a refund from their bank later.
4. Charity fraud – The victims receive text or email messages asking for donations to any number of organizations.
5. Job scam – Fraudsters pretend that they are employers and post about recruitment on online platforms. When job seekers contact fake employers, the latter might persuade them to apply for the position, but application fees are required.
6. Unexpected prize scam – The victims receive an email informing them that they have won a prize from a competition, but some fees need to be paid in advance to claim this prize.

METHODOLOGY

Data collection

The population in this study is people who have used smart phones and have experienced internet fraud, and the sample group consists of 1,224 internet fraud victims selected through convenience sampling. An online survey is the tool used for data collection in this study. The dependent variable is the value of damage (in Thai baht) caused by six common types of internet transaction fraud based on the Northern Territory Government of Australia's (2015) definitions: text message scam (smashing); online shopping scam; credit card fraud; charity fraud; job scam; and unexpected prize scam. The independent variables are divided into two groups: 1) demographic factors,

including gender, age, education level, average monthly income and marital status; and 2) internet use behaviour, including the average time spent accessing the Internet, places used as an internet access point, devices used to access the Internet and social media platforms. The covariance's in this study are the perception of benefits and the perception of security in conducting online transactions. The inferential statistic used to test the hypothesis is analysis of covariance or ANCOVA.

Data analysis using analysis of covariance (ANCOVA)

ANCOVA allows the inclusion of one or more continuous variables in addition to the variables of interest. ANCOVA is an extension of ANOVA; therefore, it can access the main effects and respond to the research hypotheses of ANOVA. A covariate, which is correlated with the dependent variable, is included in ANCOVA, and it has an influence on the means of the dependent variable adjustment (Tabachnick and Fidell, 2019). In this research, the independent variables, demographic factors and the behaviour of internet users, are group variables, and they are continuously variable, while the dependent variable, the damage value, is a discrete variable or a numeric variable; hence, ANCOVA is selected for this study to analyse the data.

RESULTS

Estimation of the total value of damage

The dependent variables' means indicate that the total value of the damage caused by all six types of internet fraud equals 3,762.95 baht per user. Online job scams cause the most damage, accounting for 990.60 baht per person. The damage due to credit card fraud has the second-highest value among smart phone users, amounting to 743.06 baht per person, followed by the damage caused by unexpected prize scams, accounting for 690.36 baht per person. The damage due to online shopping scams and charity fraud accounts for 604.04 baht per person and 442.83 baht per person, respectively. Text message scams cause the lowest value of damage to internet users, equal to 274.55 baht per person.

Tests of the group one independent variables (demographic factors)

The covariance test of the group one independent variables(demographic factors) conducted using Levene's test reveals that the variances of the within-group independent variables (demographic factors) have significant differences at the significance level of 0.05 ($F(24, 1{,}199) = 2.986$, $p = 0.000$),leading to violations of the ANCOVA assumptions ($p < 0.05$). When the sample size is larger (Shieh, 2020), it can decrease the significance level or reduce the residual error. Therefore, the study used a data set of 1,224, which is larger than the minimum sample (400 cases).

Groupone's independent variables (demographic factors) include gender, age, education level, career and income. The results in Table 1reveal that age and income affect

the total value of damage caused by internet scams at the significance level of 0.05. The changes in the independent variable with an r-squared of 0.086 ($r^2 = 0.086$) mean that the independent variable, demographic factors, can explain6.6% of the dependent variable, total value of damage caused by internet scams, with this existing variance.

Table 1: Test of the effect on the group one independent variables (demographic factors) by tests of between-subjects effects

Source	Type III sum of squares	df	Mean square	F	Sig.	Partial eta squared
Corrected model	6384220538.900(a)	33	193461228.452	3.381	0.000	0.086
Intercept	202983154.406	1	202983154.406	3.547	0.060	0.003
Age	2502153414.111	4	625538353.528	10.932	0.000	0.035
Income	2870213705.112	4	717553426.278	12.540	0.000	0.040
Age * income * perception of benefits * perception of security	5152194444.793	25	206087777.792	3.602	0.000	0.070
Error	68090545943.433	1190	57218946.171			
Total	91645479375.000	1224				
Corrected total	74474766482.333	1223				

Note: Dependent variable: total value of damage caused by internet transaction fraud.

(a) The r-squared equals 0.086,and the adjusted r-squared equals 0.060.

For this examination, the results in Table 2 show that the mean of the damage values among the internet fraud victims aged under 20 years is the highest, accounting for 10,323.336 baht, while the mean of the damage values in the age group 31–34 years is the lowest, amounting to 2,200.512 baht.

Table 2: Total value of damage categorized by age groups

Age group	Mean	Std error	95% confidence interval	
			Lower bound	Upper bound
Under 20 years old	10323.336(a)	1761.074	6868.181	13778.491
21–30 years old	8039.897(a)	951.420	6173.250	9906.544
31–40 years old	2200.512(a)	1731.392	-1196.409	5597.433
41–50 years old	1486.906(a)	1780.244	-2005.861	4979.674
Over 50 years old	3965.387(a)	2279.047	-506.012	8436.785

Note: Dependent variable: total value of damage caused by Internet transaction fraud.

(a) In this model, the existing covariates are measured based on these two values: perception of benefits = 4.1716 and* perception of security = 4.4083.

Table 3 shows that the mean of the damage values among the group of online scam victims earning incomes of 30,001–40,000 baht monthly is the highest, accounting for 10,882.869 baht, while that of the group of victims earning incomes of 10,001–20,000 baht monthly is the lowest, amounting to 2,859.020 baht.

Table 3: **Total value of damage categorized by incomes**

Income	Mean	Std error	95% confidence interval	
			Lower bound	Upper bound
Under10,000 baht	4163.473(a)	2128.659	-12.870	8339.816
10,001–20,000 baht	2859.020(a)	1044.648	809.464	4908.577
20,001–30,000 baht	3584.544(a)	2056.900	-451.010	7620.099
30,001–40,000 baht	10882.869(a)	2032.116	6895.939	14869.799
Over40,000 baht	4526.130(a)	1211.283	2149.643	6902.618

Note: Dependent variable: total value of damage caused by internet transaction fraud.
(a) In this model, the existing covariates are measured based on these two values: perception of benefits = 4.1716 and* perception of security= 4.4083.

Tests of the group two independent variables (behaviour of internet users)

The covariance test of the group two independent variables(behaviour of internet users),carried out using Levene's test, shows that the variances for the group two independent variables (behaviour of internet users) are not equal at the significance level of 0.05 ($F(5, 1{,}218) = 2.811$, $p = 0.016$),leading to violations of the ANCOVA assumptions ($p < 0.05$). When the sample size is larger (Shieh, 2020), it can decrease the significance level or reduce the residual error; therefore, the study used a data set of 1,224, which is larger than the minimum sample (400 cases).

The group two independent variables (behaviour of internet users) include the average time spent accessing the Internet, the places used as the internet access point, the devices used to access the Internet and social media platforms. Table 4 shows that only devices have a significant influence on the total damage at the significance level of 0.05. The changes in the independent variable with an r-squared of 0.066($r^2 = 0.066$) mean that the independent variable, the behaviour of internet users, can explain6.6% of the dependent variable, the total value of damage caused by internet scams, with this existing variance.

Table 4: Test of the effect among the group two independent variables (behaviour of internet users) by tests of between-subjects effects

Source	Type III sum of squares	df	Mean square	F	Sig.	Partial eta squared
Corrected model	4887759889.173(a)	11	444341808.107	7.739	0.000	0.066
Intercept	4180670953.878	1	4180670953.878	72.815	0.000	0.057
Social media platforms	4407314312.673	5	881462862.535	15.352	0.000	0.060
Social media platforms *perception of benefits *perception of security	3399480848.000	6	566580141.333	9.868	0.000	0.047
Error	69587006593.159	1212	57415021.942			
Total	91645479375.000	1224				
Corrected total	74474766482.333	1223				

Note: Dependent variable: total value of damage caused by internet transaction fraud.
(a) TheR-squared equals 0.066, and the adjusted r-squared equals 0.057.

For this examination, the results in Table 5 show that the mean of the damage values among Instagram users is the highest, accounting for 4,387.364 baht, while the mean of the damage values among blog/Google+ users is the lowest, amounting to 3,045.200 baht.

Table 5:Values of damage categorized by social media platforms

Social media Platforms	Mean	Std error	95% confidence interval	
			Lower bound	Upper bound
Facebook	3745.186(a)	292.762	3170.810	4319.562
Line	3294.266(a)	799.635	1725.444	4863.088
YouTube	4044.126(a)	406.190	3247.213	4841.039
Instagram	4387.364(a)	5121.259	-5660.153	14434.881
Blog/Google+	3045.200(a)	1288.894	1458.859	6516.280

Note: Dependent variable: total value of damage caused by internet transaction fraud.
(a) In this model, the existing covariates are measured based on these two values: perception of benefits = 4.1716 and* perception of security = 4.4083.

Value of economic damage

The economic damage in this study was evaluated following Equation 1, based on the study by Phakhinsitthinan and Kraiwanich (2017).

Equation 1:

Damage (Y)= mean of individual damage (mean) * number of Thai internet users (n)

According to Table 1, the value of damage equals 3,762.95 baht, and the number of Thai internet users based on the statistics in 2018 is 57 million users (WP, 2018); therefore, the economic damage based on this examination can be calculated as shown in Equation 2.

Equation 2:

$$\begin{aligned} Y &= 3{,}762.95 \text{ (baht)} * 57{,}000{,}000 \text{ (users)} \\ &= 241{,}488.2 \text{ million baht or US\$7,149.6 million} \end{aligned}$$

DISCUSSION

Based on the findings, demographic factors, age and income are associated with being harmed by internet transaction fraud. This study shows that adults aged over 30 tend to lose less money from internet scams than the younger groups, particularly victims under 20 years old, who lose the largest amount of money to internet fraud. However, it cannot be concluded that age is a significant factor related to the value of damage caused by cybercrimes because there are fluctuations between the total value of damage and the age groups. The study by Choi, Choo and Sung (2016) explored the relationship between age differences and computer crime victimization, and they concluded that age differences do not affect computer crime victimization and security management. Their findings explain that older adults are less likely to implement computer security software, which means that the level of online protection decreases as age increases. Moreover, older internet users are less likely to stay online for a long time; hence, they might have fewer chances of participating in risky online activities.

In this study, the use of Facebook related to the value of damage caused by internet transaction fraud. In other words, Facebook users are more likely to be harmed by online scams than users of other social media platforms. This is in line with the study by Benenson, Gassmann and Landwirth (2017), who found that 43% of Facebook users clicked on simulated phishing links. There are three reasons for this: first, Facebook is considered to be trustworthy by users; second, Facebook's special characteristics, such as easy access to an acquaintance's profile, might make the phishing links plausible; third, messages on Facebook can be checked quickly by scrolling the screen through Facebook's timeline, which is different from checking email; therefore, many notifications will be scanned quickly and a scam link might be hit accidentally.

CONCLUSIONS

Based on this study, the economic damage caused by internet transaction fraud is

more than US$7,000 million, and the top three online scams creating the highest damage values are job scams, credit card fraud and unexpected prize scams. Job scams can steal the most money from smart phone users because people are likely to trust job emails and are more likely to click on the phishing links. Credit card fraud causes huge damage to internet fraud victims since credit cards are a common method used to purchase online goods and services by many internet users. Fraudsters might hack the security code when the payment has been made or send a scam link to the victims to steal their password or security code. Unexpected prize scams can lure many victims as people love effortless rewards and prizes, especially free ones. People in the middle-age group are less likely to be attacked by internet fraud. This might be because people in this age group are considered to have high levels of intelligence, leading to good decision making. Hence, middle-aged internet users may not be particularly at risk of cybercrime attacks.

Recommendations

1. Public sectors can apply these findings to create policies regarding internet fraud prevention. For example, they can disseminate information about the perception of online transactions' benefits, ways to conduct financial transactions wisely and ways to avoid internet scams.Hence, the damage caused by internet fraud will decrease significantly.
2. Private sector security is another factor to which users pay attention, so internet users should be careful about revealing personal information via online platforms and double-check all the information in financial transaction items before the confirmation of a transaction to prevent damage caused by fraudulent transactions.
3. Providers should improve cyber security systems to support the use of internet banking, online banking and other online platforms, such as online shopping websites and chat box applications, which need to be concerned about security system development as well. For example, the most up-to-date security software should be implemented in the operations system.

Limitations

The damage caused by online fraud in this study could not be defined by frequency or risks. It is unclear whether the victims lost money only once or whether they had been cheated once per month; it is also unclear whether the risks were only identified when conducting transactions or whether they had occurred in other areas. Hence, the quantity of damage in this study is estimated. This means that the quantity and characteristics of damage in future examinations might be different from those in this study due to the fact that criminals are likely to change their fraud patterns since the old patterns can be widely detected.

References

Association of Certified Fraud Examiners. (2019).*Anti-fraud technology benchmarking report*. Texas: ACFE.

Benenson, Z., Gassmann, F. and Landwirth, R.(2017). *Unpacking spear phishing susceptibility, targeted attacks workshop at Financial Cryptography and Data Security 2017*. Malta: Springer.

Chogo, P. J. and Sedoyeka, E. (2014). Exploring factors affecting mobile money adoption in Tanzania, *International Journal of Computing and ICT Research*, 8(2), 53–64.

Choi, K., Choo, K. and Sung, Y. (2016). Demographic variables and risk factors in computer-crime: An empirical assessment, *Cluster Computing*, 19(1), 3–11.

Corbet, S., Cumming, D., Lucey, B. M., Peat, M. and Vignec, S. A.(2019). The destabilizing effects of crypto currency cyber criminality, *Economics Letters*,191.

Northern Territory Government of Australia. (2015, June 11). *Ten most common types of scams*. Retrieved from https://nt.gov.au/law/crime/scams/ten-most-common-types-of-scams.

OECD. (2014). The digital economy, new business models and key features, In *Addressing the Tax Challenges of the Digital Economy*, (pp. 69–97). Paris: OECD Publishing.

Ozturk, A. B., Bilgihan, A., Salehi-Esfahani, S. and Hua, N.(2017). Understanding the mobile payment technology acceptance based on Valence Theory: A case of restaurant transactions, *International Journal of Contemporary Hospitality Management*, 29(8), 2027–2049.

Phakhinsitthinan, P. and Kraiwanich, T. (2017). ธุรกิจใต้ดินในเศรษฐกิจดิจิตอล [Underground business in digital economy],*วารสารวิทยาลัยสงฆ์นครลำปาง* [Nakhon Lampang Buddhist College's Journal],6(1), 35–40.

Shaikh, A. and Karjaluoto, H. (2015). Mobile banking adoption: A literature review, *Telematics and Informatics*,32(1), 129–142.

Shieh, G. (2020). Power analysis and sample size planning in ANCOVA designs, *Psychometrika*, 85, 101–120.

Songwanich, S. (2016, May 22). *China's race to become a cashless society*, Retrieved from https://www.nationthailand.com/opinion/30286476.

Tabachnick, B. G. and Fidell, L. S. 2019. *Using multivariate statistics: 7th edition*. New York: Pearson.

Wang, D., Xiang, Z. and Fesenmaier, D. R. (2014). Smartphone use in everyday life and travel, *Journal of Travel Research*,55(1), 52–63. DOI: https://doi.org/10.1177/0047287514535847.

WP. (2018, February 1). *สถิติผู้ใช้ดิจิทัลทั่วโลก "ไทย"เสพติดเน็ตมากสุดในโลก – "กรุงเทพ"เมืองผู้ใช้ Facebook สูงสุด* [Statistics of global digital users, Thailand's Internet addiction shows the highest rank – Bangkok, the highest-Facebook-user city], Retrieved fromhttps://www.brandbuffet.in.th/2018/02/global-and-thailand-digital-report-2018/.