Individual Awareness of E-Wallet and Bank Staff Related Fraud in Malaysia, in the Face of Widespread Global Digitalization

Anthony Vaz[#1], Reynold Tom Fernandez[#2], Shaheen Mansori[#3], Dinesh Rao[#4]

[#1]*School of Transport & Logistics, Malaysia University of Science and Technology, Petaling Jaya, 47810, Selangor Darul Ehsan, Malaysia*

[#2]*Faculty of Business and Communication, Inti International University, Persiaran Perdana BBN, Putra Nilai, 71800 Nilai, N. Sembilan, Malaysia*

[#3]*School of Business, Malaysia University of Science and Technology, Petaling Jaya, 47810, Selangor, Malaysia*

[#4]*Faculty of Post Graduate Studies, Brickfields Asia College, B-2, G Floor, Jalan Utara, Section 14, 46200, Petaling Jaya, Selangor Darul Ehsan, Malaysia*

[1]anthony@must.edu.my
[2]reynoldtom.fernandez@newinti.edu.my
[3]shaheen.mansori@must.edu.my
[4]krishdd23@gmail.com

***Abstract*— The digitalised world is accelerating at a tremendous pace. Many banks and businesses today offer e-wallets as a way of paying bills. As more and more products and services are being offered online at just a click away, a major concern is the security and privacy of data that is widely being transmitted across cyberspace to support online businesses and payment activities. This is because, there are many cybercriminals who attempt to use methods to make financial gain from unsuspecting online users of apps. There is a wide array of apps available to users including the popular e-commerce applications, ride hailing apps, banking apps, travel apps, chat and social apps and many of these apps are used by cybercriminals, who plant links in such apps to trick users. The aim of this research is to gather information on the extent of e-wallet fraud and whether respondents have heard of bank staff being involved in fraud with objective of creating awareness on how the public can be more aware of the pitfalls of using e-wallet and banking online applications for day-to-day transactions, particularly through the use of the mobile phone to make a transaction.**

Keywords—*bank staff related online fraud, confidential information, data breach, digitalization, e-wallet fraud.*

1. Introduction

Two decades have passed in the new century and lifestyles are becoming more and more digitalized. An individual can shop for daily essentials and clothes online, order his favourite food online, hail a ride, make travel plans online, make a banking transaction and complete tax returns online [1]. Much of the new businesses are for millennials who are tech savvy and use their mobile phones for many online transactions [2]. Millennials can be defined as people born from around the mid-1990s to 2000s and are the very people who are entering the workforce now. They are the new generation of people impacting the new economy and millennials today will soon acquire inheritance from Baby Boomers and Gen X [3]. These millennials and indeed Gen X (born 1980s to mid-1880s), make up the people of society today, who use the smartphone as an important accessory in their lives. Every-day, the smartphone is used to download apps and personal data is entered to install an app. These users then make online transactions and much personal confidential data can fall into the wrong hands and result in personal financial losses [4].

2. Literature Review

Recent collapses of massive traditional businesses such as Thomas Cook and Forever 21 shows fast changing trends in how people, particularly millennials and Gen X, are now turning towards online sites for their travel, retail and other needs [5].

2.1 Estimate of volume transacted globally in e-commerce businesses

Due to the internet, e-commerce business models have grown dramatically in the last decade or so. Part of the reason besides internet penetration, is because the logistics industry has kept pace with the growing demand of physical products and services, with cloud computing, internet of things and big data propelling businesses. The list of online transactions have grown exponentially and we can see many players in the e-commerce industry grow their businesses at a remarkable pace (Figure 1).

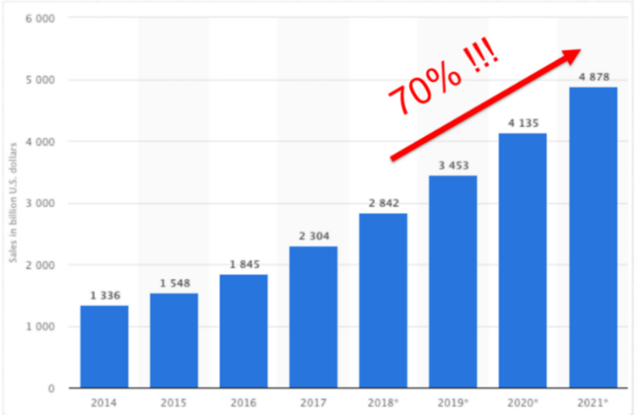

Figure 1. Growth of e-commerce globally, Source [6]

2.2 The widespread use of mobile apps in modern society

With the internet having passed its' 30 year in existence, and with internet connectivity having moved to 5G accessibility, a new society has emerged where we are a widely connected species. 5G is the fifth generation technology standard used in broadband cellular networks and provides high speed connectivity to mobile phones and laptops.

We have seen Uber and Grab using digitalization and the internet which allows not only online ride hailing but also food and other services to be delivered to the door step of a customer. Booking a ticket from an airline [7]. or purchasing bus tickets or movie tickets online [8], has never been easier and provides huge convenience to the general public at large. One can also pay for parking tickets or summonses online these days [9]. A busy executive can make an online personal tax submission and the list of applications available are endless. However, there is a dark side to all this, confidential data required when using such applications can fall into the wrong hands of cybercriminals, who may use the information to trick or fool users of such applications into parting with their money.
The types of information stolen are tabulated in (Table 1).

Table 1. Key information stolen, Source [10]

Type of information	
1.Member name	2.Mailing and/or physical address
3.Date of birth	4.Telephone number
5.Social security number	6.Banking account number
7.Member identification number	8.Clinical information
9.Email address	10.Claims information

Although we hear news daily about breaches of data, protecting user data has become increasingly important despite regulation implementation. There are numerous reports that scammers of fake accounts attempt to trick mobile phone users into revealing confidential information who subsequently incur personal losses. When we use e-commerce apps to make purchases or when we purchase travel tickets online, personal information is requested and a fake website posing as the organization may take advantage of an unsuspecting user. There is a greater need for proper infrastructure and guidelines to prevent cases such as these, because our world has changed to a society where almost everyone holds a mobile phone everywhere that person goes. Transactions can be done anywhere at the click of a finger and this poses real threats to society. Banking information must be secure, chat app users need to be aware when identity theft occurs because the unsuspecting individual will fall prey to a cybercriminal who may pose as a fake bank officer, for example. There have been reported cases on people being duped into transferring funds by such cybercriminals [11].

3. What needs to be done by individuals to be aware of the threat posed by lack of cybersecurity awareness

Studies have shown that cybercriminals exploit human curiosity that leads them to click on links in emails, download and install software, that then request for information [12], leading to money being lost! Most cybercriminals upon obtaining confidential data from data breaches, target the average unsuspecting person. Reports have shown that 99% of emails distributing malware from 2018 to 2019 required some form of human interaction to click links, open documents, accept security warnings or complete tasks to effectively compromise financial information [13].

Additionally, the use of SIM cards in mobile phones poses a threat. SIM stands for a Smart Card Inside your mobile phone. The SIM-card contains an identification number unique to the owner and stores personal data which prevents operation of the phone if the SIM-card is removed. Most systems send a verification code to your mobile phone to confirm you are the real person doing a transaction and there have been cases of cybercriminals cloning sim-cards to obtain the verification code [14].

When personal records are part of the information stolen from big companies, people are at risk, because by using personal details, cybercriminals may be able to make fake transactions for say either an e-commerce purchase or financial transfer of funds. When anyone detects that SIM-cards are being cloned, the steps to take are:

- Notify your telecommunications provider immediately.
- Notify your bank and change Personal Identification Number (PIN) codes.
- Never use your credit card to pay courier company representatives visiting you at home because these personnel might be in disguise as courier service personnel.
- Verify email addresses from incoming emails as cybercriminals may use fake accounts.

Always be wary of clicking suspicious looking links. Never download files from unknown sources. If credentials of financials have been tampered with, contact the breached company and ask for assistance in enrolling you to a fraud victim assistance program.

4. Methodology

To determine the extent of e-wallet fraud and bank staff related fraud, an online questionnaire was designed to collect information from respondents from millennial and Gen X age group. Once the data was collected, descriptive analysis was used to determine gender and age group of respondents. Cross tabulation analysis was also used to gain insights into whether respondents had heard about e-wallet fraud, bank staff related fraud as well as whether respondents would click on suspicious links on their phone or laptop and whether respondents knew fully what to do when they encountered internet related cybercrime.

5. Findings

A total of 189 respondents responded. Table2 and Table 3 shows the gender and age distribution of respondents. It is sheer co-incidence that the frequency of Male/Female and 18-22/23-38 age group, are the same.

Table 2. Respondents by gender

Gender	Frequency	Percentage of respondents
Male	70	37
Female	119	63
Total	189	100

Table 3. Age Group

Age group	Frequency	Percentage of respondents
18-22	119	63
23-28	70	57
Total	189	100

From Table 4 below, we can observe that about 26% of respondents, their family or friends were victims of e-wallet online fraud.

Table 4. Self, family & friends who are victims of e-wallet online fraud

	I am a victim of e-wallet online fraud.	I have heard of a family member who has been a victim of e-wallet online fraud.	I have heard of a friend who has been a victim of e-wallet online fraud.	% of self, family & friends, a victim?
Yes	7.4%	27.5%	42.3%	25.8%
No	92.6%	72.5%	57.7%	74.2%

From Table 5 below, we can observe that about 32% of respondents, their family or friends were victims of bank staff related fraud.

Table 5. Self, family & friends who are victims of bank staff related online fraud

	I am a victim of bank staff fraud.	I have heard of a family member who has been a victim of bank staff fraud.	I have heard of a friend who has been a victim of bank staff fraud.	% of self, family & friends, a victim?
Yes	12.7%	30.7%	51.3%	31.6%
No	87.3%	69.3%	48.7%	68.4%

To two questions that asked whether they were victims of e-wallet online fraud and whether they may click on suspicious links on their phone or laptop because they were unaware what is real and what is bogus, 14.1 % of 64 respondents, that were victims of e-wallet online fraud said they would click on suspicious links on their phone or laptop. Similarly, the remaining 85.9 % of respondents, that were not victims of e-wallet online fraud said they would click on suspicious links on their phone or laptop because they were unaware of what is real and what is bogus (Table 6).

Table 6: Cross tabulated data of 'I am a victim of e-wallet online fraud and I may click on suspicious links on my phone or laptop because I am unaware what is real and what is bogus.'

			I may click on suspicious links on my phone or laptop because I am unaware of what is real and what is bogus.		
			No	Yes	Total
I am a victim of e-wallet online fraud.	No	Count	120	55	175
		% within I am not a victim of e-wallet online fraud	96.0%	85.9%	92.6%
	Yes	Count	5	9	14
		% within I am a victim of e-wallet online fraud	4.0%	14.1%	7.4%
		Count	125	64	189
		% of Total	66.1%	33.9%	100%

Generally, the study found that about 34% of respondents may click on suspicious links on their phone or laptop because they were unaware of what is real and what is bogus.

To two questions that asked whether they are victims of e-wallet online fraud and whether they know fully what to do when they encounter any internet related cybercrime, the cross tabulation data shows that 9 % of 110 respondents of e-wallet victims were not aware of what to do when they encountered internet related cybercrime. Similarly, the remaining 92 % of respondents, that have not been victims of e-wallet fraud, were also not aware of what to do when they encountered internet related cybercrime (Table 7).

Table 7. Cross tabulated data of 'I am a victim of e-wallet online fraud and I know fully what to do when I encounter any internet related cybercrime'

			I know fully what to do when I encountered internet related cybercrime		
			No	Yes	Total
I am a victim of e-wallet online fraud	No	Count	97	78	175
		% within I am not a victim of e-wallet online fraud	91.5%	94%	92.6%
	Yes	Count	9	5	14
		% within I am a victim of e-wallet online fraud	8.5%	6%	7.4%
		Count	110	106	189
		% of Total	53.4%	56.1%	100.0%

Generally, the study found that about 53% of respondents do not know fully what to do when they encountered internet related cybercrime.

To two questions that asked whether they were victims of bank staff related fraud and whether they have heard of Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010, 12 % of 84 respondents that were victims of bank staff related fraud, said they have not heard of Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010. Similarly, the remaining 88 % of respondents that were not victims of bank staff related fraud also said they have not heard of Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010. (Table 8).

Table 8. Cross tabulated data of 'I am a victim of bank staff related fraud and I have heard of Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010'.

			I have heard of Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010.		
			No	Yes	Total
I am bank staff related fraud.	No	Count	74	91	165
		% within I am not victim of bank staff related fraud	88.1%	86.7%	87.3%
	Yes	Count	10	14	24
		% within I am not victim of bank staff related fraud	11.9%	13.3%	12.7%
		Count	84	105	189
		% of Total	44.4%	55.6%	100%

Generally, the study found that about 44% of respondents have not heard about Cybersecurity Laws and Regulations & The Personal Data Protection Act 2010.

6. Recommendations for future study

There is a greater need for the citizens of Malaysia to be aware of crimes committed by cybercriminals and those with links to staff in banks. The public needs to be aware that crimes are happening through e-wallets for general public use, because the findings of this study are rather alarming. The results of this study are backed by the reports in the media that many people are being scammed almost on a daily basis. Cybercriminals continue to attack government portals and businesses that offer online products and services to the general public. Businesses that operate in huge digital data environments are at risk, even for everyday users of online applications. It was reported that Malaysians lost RM914 million to investment scams within the first six months of 2020, says the Securities Commision (SC) chairman [15. In neighbouring Singapore, a recent media report stated that more than S$201 million was cheated in the top 10 scams in 2020 of which the top four scams of concern are e-commerce, social media impersonation, loan scams and banking-related phishing scams [16]. More studies need to be conducted to spread awareness of how it can happen and what are the steps needed to prevent data breach and ultimately how users need to remedy such breaches when cybercriminals gain access to confidential personal information. A survey of users in government, industry and society at large may reveal the true extent of the problem and it is recommended as the next step in this paper.

Acknowledgments

The authors would like to thank all participants who have contributed to the publication of this article.

References

[1] Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2018). Mobile commerce and the internet of things. In *Electronic Commerce 2018* (pp. 205-248). Springer, Cham. https://doi.org/10.1007/978-3-319-58715-8_6

[2] Femenia-Serra, F., Perles-Ribes, J. F., & Ivars-Baidal, J. A. (2019). Smart destinations and tech-savvy millennial tourists: hype versus reality. *Tourism Review*. *74*(1), 63-81.

[3] Kelly, J. (2021). *Millennials will become richest generation in American history as Baby Boomers transfer over their wealth.* Forbes. Retrieved from https://www.forbes.com/sites/jackkelly/2019/10/26/millennials-will-become-richest-generation-in-american-history-as-baby-boomers-transfer-over-their-wealth/?sh=5849c41a6c4b

[4] A/P Sinnathamby Sehgar, S.; Zukarnain, Z.A. Online Identity Theft, Security Issues, and Reputational Damage. Preprints 2021, 2021020082 (doi: 10.20944/preprints 202102.0082.v1).

[5] Sidhu,B.K.(2019). *12 Industries to thrive, thanks to Millennials*, Economy, The Star Online. Retrieved from https://www.thestar.com.my/business/business-news/2019/10/05/12-industries-to-thrive-thanks-to-millennials#oDqFF8b4w3mJoHpE.99

[6] Acepro Academy (2019). *The proven E-commerce System: How Malaysians can start, sell and scale their e-business with Amazon.* Retrieved from https://aceproacademy.clickfunnels.com/5ssa-kl-proven-system-cf?target=fb-5ssakl-ecs1a1&cam=fb-5ssakl-ecs1a1

[7] Suki, N. M., & Suki, N. M. (2017). Flight ticket booking app on mobile devices: Examining the determinants of individual intention to use. *Journal of Air Transport Management*, *62*, 146-154.

[8] Islam, G., Zinnia, I., Hossain, M., Rahman, M., Juman, A., & Emran, A. (2020). Implementation of an efficient web-based movie ticket purchasing system in the context of Bangladesh. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(3), 828-836.

[9] Heffetz, O., O'Donoghue, T., & Schneider, H. S. (2020). Reminders Work, But for Whom? Evidence from New York City Parking-Ticket Recipients. *Evidence from New York City Parking-Ticket Recipients (March 26, 2020)*.

[10] Trend Micro Inc (2018). *Data breaches 101: How they happen, what gets stolen ad where it all goes* Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101?cm_re=8_17_18-_-Notification1-_-Data_Breaches

[11] RBC (2019). *How cybercriminals make contact*, Retrieved from https://www.rbc.com/cyber-security/how-cyber-criminals-make-contact/index.html

[12] Proofpoint Threat Insight Team (2019). *Pervasive social engineering characterises the threat landscape: Proofpoint releases the Human Factor 2019 report*, Retrieved from https://www.proofpoint.com/us/threat-insight/post/pervasive-social-engineering-characteristics-threat-landscape-proofpoint-releases

[13] Information Week IT Network (2019). *More than 99% of cyberattacks need victim's help,* Retrieved from https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

[14] Siciliano, R., (2019). *How hackers can drain your bank account using the SIM card scam*, Hotspot Shield, Retrieved from https://www.hotspotshield.com/blog/hackers-phone-sim-card-scam/

[15] Malay Mail (2020). *Malaysians lost RM914 million to investment scams for first six months of 2020, says SC chairman*. Retrieved from https://www.malaymail.com/news/malaysia/2020/10/23/malaysians-lost-rm914m-to-investment-scams-for-first-six-months-of-2020-say/1915544#:~:text=Malaysians%20lost%20RM914m%20to%20investment,SC%20chairman%20%7C%20Malaysia%20%7C%20Malay%20Mail

[16] Baker, J.A. (2021*). More than S$201 million cheated in top 10 scams types last year: Police.* Retrieved from https://www.channelnewsasia.com/news/singapore/more-than-201-million-cheated-top-10-scam-types-2020-police-14145720