

Vedamanikam & Chethiyar, 2020

Volume 4 Issue 1, pp. 19-37

Date of Publication: 25th June 2020

DOI- <https://doi.org/10.20319/pijtel.2020.41.1937>

This paper can be cited as: Vedamanikam, M., Chethiyar, S. D. M. (2020). Money Mule Recruitment among University Students in Malaysia: Awareness Perspective. PUPIL: International Journal of Teaching, Education and Learning, 4(1),19-37.

This work is licensed under the Creative Commons Attribution-Non Commercial 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

MONEY MULE RECRUITMENT AMONG UNIVERSITY STUDENTS IN MALAYSIA: AWARENESS PERSPECTIVE

Mohanamerry Vedamanikam

*Manager, AML Compliance, Western Union Payments (Malaysia) Sdn Bhd (970512P)
Level 22.03, The Gardens North Tower, Mid Valley City, Lingkaran Syed Putra, 59200
Kuala Lumpur, Malaysia
mohanamerry.vedamanikam@wu.com*

Saralah Devi Mariamdarani Chethiyar

*Senior Lecturer, Psychology & Counselling Program, School of Applied Psychology, Social Work and Policy, College of Arts and Sciences, University Utara Malaysia, Malaysia
devi@uum.edu.my*

Abstract

Money laundering is perceived as a global threat with funds sourced from illegal and fraudulent activities. Money mules are recruited by criminal networks in money laundering chain, positioned between actual criminal and the illicit funds, enabling the criminals to be anonymous and non-visible to the detection of law enforcement. Job vacancy with various positions are offered with attractive financial rewards and work flexibility and the criminal elements are hidden behind the job criteria. Awareness on job criteria and the hidden criminal elements is a crucial factor in job acceptance. This study examines recruitment anatomy of students as money mules and job acceptance decisioning from awareness perspective. Library research methodology was employed in this research by reviewing existing research works on money mule recruitment to identify the underlying reasons and lapses in money mule recruitment and

statistical analysis on the reported money mule cases. Based on the examination, students are captivated to attractive job packages and accept the offer without being aware of the criminal activity at the background and directly expose them to enforcement actions. Incrementing statistics sets the scene of scarcity in the perspective of awareness on job criteria among students and crucial for students to assess and consciously decide on the acceptance and avoid victimized by the criminal networks.

Keywords

Money Mule, Money Laundering, Criminal Network, Money Mule Recruitment, Job Criteria, Awareness

1. Introduction & Theory

1.1 Introduction

The swift and complex digital technology in the Fourth Industrial Revolution (IR4.0) have enormously impacted conventional industries, forcing quantum leap from science fiction to science fact. The exponential growth in digital platform has gain traction from digital or cyber criminals, abusing the digital platform for financial crimes victimizing consumers and resulting in financial loss (Bernama, 2019a). Unlawful proceeds for these crimes enter money laundering cycle to distort the trail of the illegal activities. Money laundering is a financial crime which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source (MatIsa, MohdSanusi, Haniff & Barnes, 2015). To maintain anonymity, money mules are individuals recruited by the criminals and fraudsters to use their personal banking account as intermediary account to interrupt the trail of the illegal funds. Criminals portray them as recruiters and offer job opportunities and lure their candidates with attractive financial rewards for them to accept the offer. The victims are visible to the law enforcement and face the consequences (Arevalo, 2015; Barclays, 2019; Charles, 2014; DeSantis, Dougherty, McDowell, 2013; Europol, 2019b; Leukfeldt & Jansen, 2015). Money mules have become an emerging threat globally allowing the actual criminals to be undetected and incurring massive financial loss.

1.2 Motivation

According to Thomson Reuters a steady growth has been reported in financial crime in the recent years resulting in financial loss where, in 2018 the estimated loss was USD1.45 trillion from the overall global economy and USD166bil from Asia Pacific economy (Thomson Reuters,

2019). In Malaysian context, Ministry of Communication and Multimedia have indicated that cybercrimes in Malaysia have recorded total loss of RM398.6 million in 2018 and subsequently in 2019, between January and May, the total loss was recorded as RM153 million, which accounted for 38 per cent of the total loss in 2018. For the similar duration in 2019, a total loss of RM40.7 million was recorded for e-financial fraud which has tremendously exceeded total loss recorded for entire 2018, RM40.5 million. In the first quarter of 2019, 2,207 cybercrimes were reported and resulted in loss of RM67.6 million. 3 most cybercrimes recorded were cheating via telephone calls, cheating via online purchases and African Scam. Ministry also indicated that cybercrimes impose serious threat to the people, causing them to lose their hard-earned money. (Bernama, 2019b, Bernama, 2019c).

National Risk Assessment (NRA) is a report published by Central Bank of Malaysia (known as Bank Negara Malaysia or BNM) based on the assessment of prevailing crimes and vulnerabilities to money laundering and terrorism financing risks. In NRA 2013, fraud was identified as one of the criminal activities with ML threat that has potential to generate illicit funds, contributed by deposits involving account mules (Bank Negara Malaysia [BNM], 2013). In NRA 2017, fraud has been reported as the highest inherent risk by the central bank with money mule as the highly observed crime and risk (BNM, 2017). Aligned to this, the analysis of Royal Malaysia Police (RMP) commercial crime investigation department reported that the number of mule accounts had increased almost eight-fold since 2015 (Royal Malaysia Police, 2018).

BNM's LNK and Regional Offices director Datin Arlina Ariff mentioned in an interview that students from higher learning institutions (IPT), have become main target for money mule by Macau Scam syndicates. The criminals attracted the students with large amount of money as 'payment' for using their identity to open bank account for the third parties. It was also mentioned that the students were tricked by the tactics due to the desire to earn easy money to cover daily expenses (Bernama, 2019e).

Between December 2018 and January 2019, RMP has detained 145 individuals which was comprised of 90 male and 55 female foreign nationals and locals nationwide suspected to have allowed their bank accounts to be used by third parties. The suspects were between the age of 19 and 63 and were mostly students, retirees and drug addicts. The suspects were introduced to unknown individuals via social media sites, thereafter they handed over their ATM cards and

personal identification numbers (PIN) to a syndicate, mentioned for business dealings (Bernama, 2019d).

1.3 Related Theory

According to Fischer, Lea and Evans (2013), theory of Heuristics, social influence and individual differences explains four key reasons for any individual respond to fraudulent communication which is applicable for this study. Motivated due to magnitude of the reward, trust built on interaction instead of message content and message origination, social influence, and the urgency of the opportunity are the key reasons of this theory which greatly related to the decision of students in accepting job offers.

1.4 Problem Statement

The increase in financial losses due to money laundering, fraud and cybercrime activities and the increase in money mules indicating the worsening situation, thus this alarming phenomenon need to be examined. Students are found to be favorite targets of criminal networks, taking advantage on their financial needs. Money mulling is being offered as job opportunity with attractive rewards, blinds to the students to the criminal element behind the scene. It is vital to examine the understanding and mindset of students on the job criteria which makes them vulnerable to accept job offers from criminals and awareness program on job criteria as prevention catalyst for this phenomenon.

1.5 Significance of the Study

The outcome of this research is expected to benefit Ministry of Education in reviewing and expanding the National Education Policy and curriculum to include digital criminology in the curriculum as futuristic initiative. It is also a timely action for Communication and Multimedia ministry and the mobile and internet technology players to review the existing polices for students' mobile data plans, usage of internet and close monitoring on the prohibited websites and social medial networks. This research is expected to facilitate Ministry of Human Resource to expand the governance on job offering, recruitment process and establish helpdesk for students. The outcome of this research also to benefit financial industry players and digital economy policy makers to define money mule crime as an interruptive parameter by including the money mule behavioral aspect in big data analytics, machine learning and monitoring to detect suspicious activities.

1.6 Scope and Limitation

Tertiary education students between the age of 19 to 34 would be the potential candidate group for this research. Accurate information is crucial in this research as some students may not provide complete and accurate information due to the fear of exposing their personal information and in certain cases their involvement with criminal networks.

2. Literature Review

2.1 Money Laundering

Financial motive is a common denominator for most of the crimes. Smuggling, illegal arms dealings, drug/human/wildlife trafficking, fraud, corruption, and cybercrimes such as email spoofing, cyber terrorism, cyber pornography, malware, ransomware, identify theft, denial of service, online scam and phishing are among the crimes that generates massive illicit funds. The money trail is evidence of their crime and illegal activities. Money-laundering scheme disconnects and disguises illicit funds from original source without compromising the criminals who wish to benefit from the proceeds. According to United Nations Office on Drugs and Crime, amount of money laundered annually estimated between 2 – 5 % of global GDP (USD 800 billion – USD 2 trillion) (Europol, 2019c; Financial Action Task Force, 2014; United Nations Office on Drugs and Crime, 2020). (Banday, 2011). Europol, the law enforcement agency for European Union, in the fifth European Money Mule Action (EMMA 5) which took place between September – November 2019 reported that 90% of money mule cases were linked to cybercrime (Europol, 2019b).

Macau scam, Credit Card Fraud, E-Banking Fraud, Inheritance Fraud, Insurance Fraud, International Scam, Love Scam, Parcel Scam are among the fraudulent activities in Malaysia causing victims lose their money. The criminals will call the targeted victims and pretend to be police/central bank/court/custom officer and traumatize the victim with crimes that they never involved. To avoid legal actions, the victim will be asked to transfer a sum of money into bank account belong to the money mules. (Royal Malaysia Police, 2019).

Malaysian Computer Emergency Response Team (MyCert) is a service delivered by Cybersecurity Malaysia consists of specialist of various cybersecurity areas and provides emergency response to computer security related incidents. Between 2017 till 2019, fraud and intrusion seem to be the most reported incident. Within this period, maximum cases for fraud

increased from 500 to 1000 (Malaysian Computer Emergency Response Team, 2019). Throughout 2019, fraud is the highest reported incident, giving indication on the increase of fraudulent activities.

2.2 Money Mules

Money mule is a character not part of the criminal network but hired by criminal network and positioned within the criminal network to diversify the trail of the enforcement agencies. They interrupt the money trail while the criminal benefits from laundered funds. Money mule receives money from a third party in their bank account and withdraws the cash or transfers the funds to another account and receives commission for the transfer. Apart from self-operating, mules open bank accounts or businesses under their names which will be operated by the criminal networks to launder the money. Money mules are accomplices in the criminal activity as they launder the illegal funds. Compared to the risk taken by the money mule, the reward is relatively low. (Aston et al., 2009; Australian Institute of Criminology, 2017; DeSantis et al., 2013; Europol, 2019b; Leukfeldt, 2014; Leukfeldt & Jansen, 2015; Leukfeldt & Kleemans, 2019).

Most of the money mules were young people with no prior knowledge of illicit behavior and assumed it was a legitimate job. According to Europol (2019b), unemployed, students and those with desperate financial situations become easy targets of criminals. Individuals between the age of 15 – 44 seem to have active participation in money muling, with individuals between the age group 24-34 having the highest participation (Aston et al., 2009; Leukfeldt & Jansen, 2015).

Cost of study in public and private universities are on the rise, indirectly causing an increase in the cost of living. Students in universities highly depend on funds from parents, study loans and scholarships. No external funding, delayed loan/scholarship or insufficient loan/scholarship forces students to look for alternate methods to earn money (Daud, Norwani, & Yusof, 2018). The financial strain and imbalance create the situation for the students to look out for job opportunities that suit their timetable. Jobs offered by money mule recruiters receive their attention due to the nature of flexible, attractive salary and rewards and all the tasks done online.

2.3 Internet and Social Media

Internet and social networks have become a conduit for criminal networks to anonymously target the victims by offering jobs or establishing relationships. Between January and March 2019, Facebook removed more than 2 billion fake accounts (Silverman, 2019). This is a significant volume that rings the alarm that any “friend request” from known or unknown names might be

fake account with fake name, photo and profile details. Similar trend is applied by criminals in creating fake company profiles and advertise job vacancies.

Based on research conducted in Jazan University, Saudi Arabia, majority of students spend more than 4 hours in social networking and feel depressed if the social network is not available (Khormi Ageel, Otayf, Al-Shafai, Majrashi & Hakami, 2016). Students were using social media for purchasing, business opportunities, advertisement, finding social contacts, finding jobs and time passing (Shafique, Anwar & Bushra, 2010).

As of January 2019, in Malaysia reported as 40.24 million mobile subscribers which is 125% penetration rate of overall population of 32.4 million reported for 2018. On average Malaysians spend daily 8 hours and 5 minutes online and almost 3 hours in social media (Bernama, 2019f). In the annual survey conducted by Malaysia Communications and Multimedia Commission (MCMC), the following findings emerged in the 2018 (Malaysia Communications and Multimedia Commission, 2019):

- Internet users increased from 24.5 mil (76.9%) in 2016 to 28.7 mil (87.4%) in 2018, which is more than 10% increase.
- Smartphone being the most common device to connect to internet (93.1%)
- WhatsApp and Facebook were the most popular communication and social networking platform
- Online banking users increase from 41.7% in 2016 to 54.2% in 2018
- Internet users between age group 20 to 30 concur the usage of internet more than 55% and consume the platform for more than 7 hours daily
- 27.5% of online activities were related to job application.

Criminal networks observe the activities of their targeted victims in the internet platform and social network and approach them to be recruited as money mules.

2.4 Recruitment of Money Mules

2.4.1 Money Mule Recruited Cases

The first money mule case was reported in Australia in January 2005 which involved 61 individuals who were recruited as part time workers and promised up to \$4,000 monthly. Their job was to perform wire transfer on the funds transferred into their accounts to accounts located at overseas. They were transferring up to \$100,000 daily and collected daily wages between \$200 to \$500 (Arevalo, 2015).

In 2018, Santander UK bank conducted an experiment on money mule recruitment. They created a fictitious company called MoneySpark and advertised a job vacancy for the position of Financial Transaction Control Analyst involving 2000 individuals between the age of 18 to 55. 32% of individuals were interested to apply while 27% were willing to leave their current job. 15% were able to correctly spot the job advertisement was for money mule while 71% didn't understand the contents of the advertisement. Analyzing the situation, the head of fraud strategy of the bank mentioned that criminals target for vulnerable audience taking advantage of weak areas, in this case desperate for job (Gayle, 2018).

The first money mule case in Japan was reported in September 2013, a 57-year-old jobless man since 2012. He was offered 500,000 Japanese Yen during probation and 700,000 Japanese Yen upon confirmation. Tasks were sent via email, received from individual mentioned as his boss. First task was to conduct survey on food market, relevant to the firm's nature of business. The second task onwards he was informed that funds will be transferred into his account and within 48 hours to withdraw and transfer to the individual mentioned in the email via international fund transfer service providers. After 4 transfers, he was arrested by the local authorities and he was informed being perpetrator of money mule scam. For each transfer, he had the doubt of the funds in and funds out, but to secure the monthly income, the thoughts were outweighed (Shimbun, 2014).

2.4.2 Money Mule Recruitment Techniques

The reachability of internet and advancement of internet and mobile platforms have changed the traditional method of recruiting (Sinha & Thaly, 2013, as cited in Koch, Gerber & De Klerk, 2018). Internet and social media have been key drivers in the development of new sourcing tools and sourcing candidates (Hunt, 2014, as cited in Koch, Gerber & De Klerk, 2018). According to Barclays (2019), 57% of students were interested in job adverts that indicated no experience required while 50% were interested in offers on money earned by work from home. Face to face, online job search engines, social network and online dating websites are methods employed by criminal networks to advertise and recruit money mules. The advertisement will contain job vacancy for positions such as financial manager, account manager, money transfer manager and others (Arevalo, 2015; Charles, 2014; Dunham, 2006, as cited in Arevalo, 2015; DeSantis et al, 2013).

2.4.3 Job Criteria and Hidden Criminal Elements

Warning signs and common criteria seen in the money mule job offer and advertisement (Charles, 2014; Europol, 2019b):

- a) Promising easy money.
- b) Position involves funds and goods.
- c) Job adverts from overseas companies and interested to hire local counterparties to act on their behalf.
- d) Non organizational-based email such as Gmail and yahoo used for communication, no match to the company's name.
- e) High salary and rewards beyond expectation.
- f) Doesn't require experience in any skill set.
- g) Work from home scheme included as flexible privilege.
- h) All interactions and transactions regarding the job will be done online.
- i) Job advertisement copied from a genuine company website.
- j) The specific job functions are not described.
- k) No educational or experience requested.
- l) All communication and work tasks will be done online.
- m) Requires usage of personal bank account as part of job requirement.
- n) Unprofessional job posting with grammatical errors

Usage of public emails, not requiring educational background, disregard experience and the most critical, usage of personal bank account are among the hidden agenda on the criminal intention. Another reason, company is overseas and need representative in victim's country is a common reason given for not having face to face communication and no office presence locally. Upon the victim accepted or responded to the job offer, the below items will proceed (Charles, 2014):

- a) Provide signed contracts or agreements to create apparent legitimacy.
- b) Provide personal bank account details and open new bank accounts.
- c) The victim account will have deposit from unknown individuals, deposited as cash or account transfer.
- d) The victim will be advised on the commission and provided with instructions to transfer the funds via money transfer service providers.

e) Money transfer usually done to overseas individual or bank account.

Students are unable to understand realize the out of norms and non-legitimacy of business handling, especially using personal accounts, money deposited by unknown individuals and money transferred to unknown individuals.

2.5 Relationship Scam

Mule cases recruited via online relationship or romance scam were reported on the rise, with criminals increasingly recruiting money mules on online dating sites and social networks, cultivating relationship to convince them to perform fund transfers or open bank accounts under the guise of sending or receiving funds (Charles,2014; Europol, 2019a). The criminal elements are hidden and unseen behind the relationship. Some of the behaviors of criminals in romance scam:

- After initial conversation, the fraudster reconnects via email and messaging systems.
- Show high interest in the relationship and start using pet names.
- Away from home country but soon to be back home.
- Less information is shared about them.

Apart from romance scam, criminals turning to social media to recruit new accomplices through get-rich-quick online advertisements, lottery scam, employment scam and inheritance scam. Some of the reason given to involve victim in receiving and transfer of funds (Charles, 2014; Europol, 2019a):

- Issues with their foreign account.
- Charity or donations to certain people in victim's country.
- Huge sum inherited in victim's country and having difficulty in receiving the funds.

2.6 Awareness as Prevention Tool

Based on the study conducted on the cybersecurity behavior, students at higher learning has shown high possibilities of being vulnerable to cyber security threats which could possibly eliminated with sense of awareness of the threats. Cybersecurity knowledge and awareness education would become shield, defending the students from the evolving cybercrimes and cyberthreats (Muniandy L, Muniandy B & Samsudin, 2017). According to Latif and Abdul-Rahman (2018), lack or absence of knowledge in money laundering is seen from the aspect of understanding of financial crime, legal and related laws, and the importance of fight against money laundering and socio-economy impact when someone participates in this crime.

Awareness is considered a prevention tool that exposes the crime and prepares the consumer for the battle, which eventually will reduce the crime and victimization (Magalla, 2018).

In the case of Santander UK bank, to prevent the innocent from being victimized, raising awareness was mentioned to be the key action required (Gayle, 2018). Realizing the increasing phenomenon of money mules among students, United Kingdom (UK) Finance and Credit Industry Fraud Avoidance System (CIFAS) that provides fraud prevention services have started campaign and website that provide information and warning on being targeted by the criminals to become money mule (Middlesex University, 2019). According to Ross Martin, the head of Digital Safety at Barclays, UK, students with financial strain are being tricked by the criminals, thus it is vital for students to be provided with necessary tools and knowledge that can save the students from mulling vulnerabilities (Barclay, 2019).

2.7 Law Enforcement

BNM, RMP and the Malaysian Communications and Multimedia Commission (MCMC) are among the law enforcement agencies tasked to manage money laundering, fraud, scam and cybercrime offenses. Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA 2001) is the Malaysian law endorsed to provide measures for money laundering and terrorism financing crimes and forfeiture of the properties and proceeds from the unlawful activities. (BNM, 2019a). Section 4 of Anti Money Laundering Act (AMLA) states, upon conviction, money laundering and terrorism financing offenders will be liable for imprisonment not exceeding 15 years and fine not less than 5 times of the value of the unlawful proceeds or five million ringgit, whichever is the higher (BNM, 2019b).

3. Objective of the Study

3.1 Research Hypothesis

Recruitment is a crucial aspect in establishing role of money mule in money laundering cycle. Among the victims are students, especially universities and colleges, who look for funds to support their studies and personal expenditures. Below are the hypotheses formulated in this research:

- a. H1: Students are favorite targets of criminal networks for money mule recruitment.
- b. H2: Criminal networks employ various techniques to recruit money mules.
- c. H3: Criminal elements are hidden behind the job criteria.

- d. H4: Social media influences the decision of the students in accepting jobs offered by criminal networks.
- e. H5: Students accept job offer due to lack of awareness on the hidden criminal elements behind the job criteria.

3.2 Research Objective

This research will meet objectives stated below:

- a. To examine reason for students being favorite target of criminal networks.
- b. To examine various techniques employed by criminal networks to recruit money mules.
- c. To examine the job criteria and hidden criminal elements in the of the job offered to students.
- d. To examine the influence of social media in the decision for students to accept the job offered by criminal networks.
- e. To examine job acceptance by students due to lack of awareness on the hidden criminal elements behind the job criteria.

3.3 Research Questions

This research will respond to questions below:

- a. Why do the students have become favorite and easy targets of criminal networks?
- b. What are the recruitment techniques employed by criminal networks?
- c. What are the job criteria offered and hidden criminal elements?
- d. How does social media influence students to accept job offers?
- e. Would awareness on the job criteria and hidden criminal elements enable students to derive conscious decision in job acceptance?

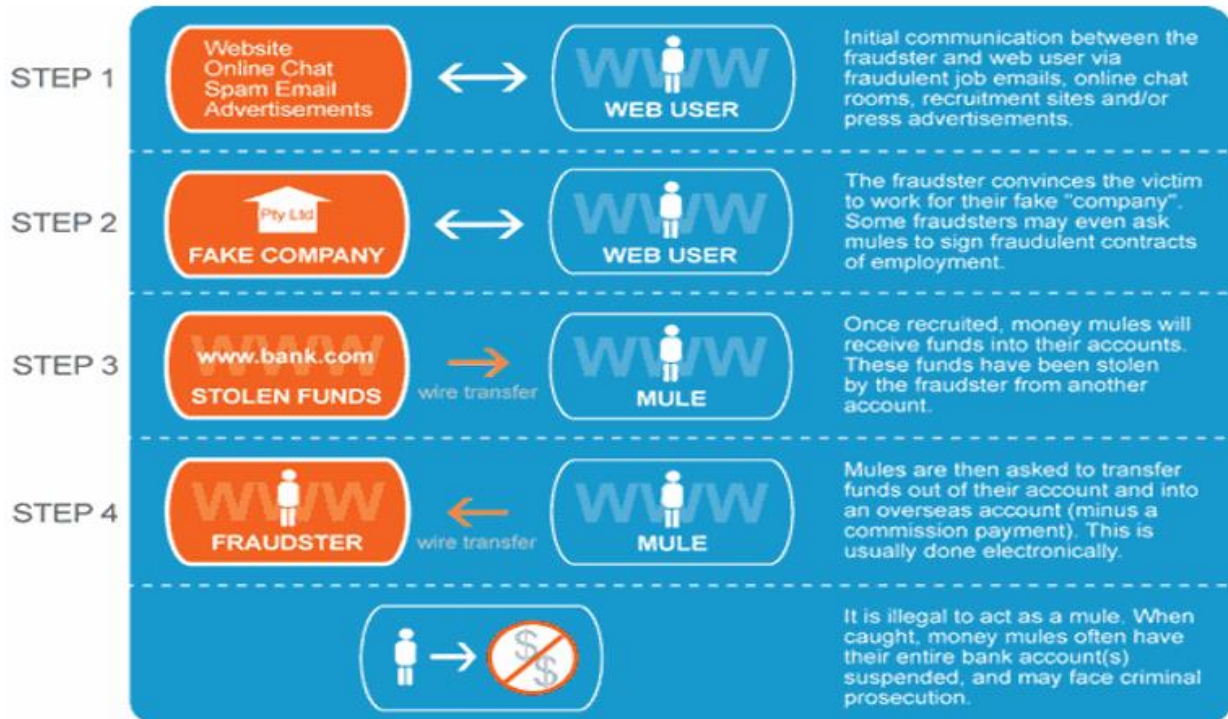
4. Methodology

Library research methodology was employed in this research. This method requires formation of questions, which leads to search of related resources and finalized with reasoned and defensible answers. Employing this approach, existing research works on money mule recruitment were reviewed and analyzed to identify the underlying reasons and lapses that resulted in successful money mule recruitment, specifically among students. This was followed statistical analysis on the cases recorded by law enforcement and experiments conducted by

financial institutions on money mule recruitment that exposed behavior in job acceptance and related statistics which affirm the existence of analogue pattern that correlates with the findings in the existing research work.

5. Conclusion and Discussion

Based on the statistics reviewed and literatures discussed, students in higher learning, with the nature of heavy internet usage and addicted to social networks, highly vulnerable to cyber threats and high potential of being victimized by criminal networks. To maintain anonymity and to be invisible to law enforcement, criminal networks recruit money mules by offering attractive job packages. The criminal elements are hidden behind the job criteria that are offered with financial income and flexibility. Students are attracted to such job packages and accept the offer without be aware of the criminal activity at the background, performs the financial transactions and directly expose them to enforcement actions. Despite having related laws and enforcement actions defined, the incremental statistics sets the scene of scarcity in the perspective of awareness on job requirements among students. Awareness and understanding on the job criteria and rewards offered are crucial for students to assess and consciously decide on the acceptance.



Source: <http://www.afp.gov.au/>

Figure 1: Online Job Scam & Money Mules (Arevalo, 2015)

This research can further expand to investigate money mule crimes involving housewives, unemployed and retirees. Other aspects such as peer influence and desperate financial strain can become parameters for future research work. Investigating if the money mule is recruited from a selected or targeted group or by random selection can be another aspect of research that can be done to expose the modus operandi of the criminal network.

6. Acknowledgment

I would like to thank Dr Saralah Devi Mariamdarani for the advice, guidance and knowledge sharing throughout the journey of this study. I also would like to thank my colleagues and family members for the encouragement and support.

REFERENCES

- Arevalo, B. C. (2015). *Money Mules: Facilitators of financial crime - An explorative research on money mules in the Netherlands*. [Master's thesis, Faculty of Law, Economics, and Governance of Utrecht University]. Academia.

https://www.academia.edu/28122208/Facilitators_of_financial_crime_An_explorative_research_on_money_mules_in_the_Netherlands

- Aston, Manny, McCombie, Stephen, Reardon, Ben & Watters, Paul. (2009). *A preliminary profiling of internet money mules: An Australian perspective*. [Paper presentation]. IEEE Xplore Symposium and Workshops on Ubiquitous, Autonomic and Trusted Computing, 2009. <https://doi.org/10.1109/UIC-ATC.2009.63>
- Australian Institute of Criminology. (2017). *Money mules*. Retrieved from <https://aic.gov.au/publications/htcb/htcb016>
- Banday. T.M. (2011). *Emerging challenges of cybercrimes to cyber security*. [Paper presentation]. International Conference on Recent Advances in Electronics and Computer Engineering, India 2011. <https://doi.org/10.13140/RG.2.1.1503.7524>
- Barclays. (2019). *Barclays issues warning to university students, as number of under-21s recruited as money mules nearly doubles*. <https://www.actionfraud.police.uk/news/barclays-issues-warning-to-university-students-as-number-of-under-21s-recruited-as-money-mules-nearly-doubles>
- Bernama. (2019a). Internet fraud and fake news on the rise in Malaysia, statistics show. *Malaymail*. <https://www.malaymail.com/news/malaysia/2019/05/17/internet-fraud-and-fake-news-on-the-rise-in-malaysia-statistics-show/1753880>
- Bernama. (2019b). The dirt on money laundering. *TheStar Business News*. <https://www.thestar.com.my/business/business-news/2019/05/25/the-dirt-on-money-laundering>
- Bernama. (2019c). RM67.6 million lost to cybercrimes in Q1 2019. *The New Straits Times*. <https://www.nst.com.my/news/crime-courts/2019/04/482208/rm676-million-lost-cyber-crimes-q1-2019>
- Bernama. (2019d). Police: 145 owners of ‘mule accounts’ detained. *Malaymail*. <https://www.malaymail.com/news/malaysia/2019/01/18/police-145-owners-of-mule-accounts-detained/1714067>
- Bernama. (2019e). Macau Scam targets IPTS students to provide ‘mule accounts’. *The Sun Daily*. <https://www.thesundaily.my/local/macau-scam-targets-ipts-students-to-provide-mule-accounts-LN681519>

- Bernama (2019f). Malaysia ranks top 5 globally in mobile social media penetration, highest in region. *The New Straits Times*
<https://www.nst.com.my/lifestyle/bots/2019/01/456119/malaysia-ranks-top-5-globally-mobile-social-media-penetration-highest>
- Bank Negara Malaysia. (2013). *Malaysia's National Risk Assessment*.
<http://amlcft.bnm.gov.my/AMLCFT03.html>
- Bank Negara Malaysia. (2017). *National Money Laundering (ML) & Terrorism Financing (TF) Risk Assessment (NRA) 2017*. <http://amlcft.bnm.gov.my/AMLCFT03.html>
- Bank Negara Malaysia. (2019a). *Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)*.
http://www.bnm.gov.my/index.php?ch=bm_legislation&lang=en AMLATFPUAA
- Bank Negara Malaysia. (2019b). *Malaysia Anti-Money Laundering & Counter Financing of Terrorism Regime*. <http://amlcft.bnm.gov.my/AMLCFT02bi.html>
- Charles, B.S. (2014). *The most common schemes for targeting the unknowing money mule*.
<https://securityintelligence.com/the-most-common-schemes-for-targeting-the-unknowing-money-mule>
- Daud, N., Norwani, N. M., & Yusof, R. (2018). Students financial problems in higher education institutions. *International Journal of Academic Research in Business and Social Sciences*, 8(10), 1558–1565. <https://doi.org/10.6007/IJARBS/v8-i10/5312>
- DeSantis, M., Dougherty, C., McDowell, M.(2013). *Understanding and protecting yourself against money mule schemes*. <https://www.us-cert.gov/security-publications/understanding-and-protecting-yourself-against-money-mule-schemes>
- Europol. (2018). *Over 1500 money mules identified in worldwide money laundering sting*.
<https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting>
- Europol. (2019a). *228 arrests and over 3800 money mules identified in global action against money laundering*. <https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering>
- Europol. (2019b). *Money mulling*. <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-mulling>

- Europol. (2019c). *Money laundering*. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering>
- Financial Action Task Force. (2014), *Money laundering FAQ*. <http://www.fatf-gafi.org/faq/moneylaundering>
- Fischer P, Lea SE, Evans KM (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *J Appl Soc Psychol* 43(10): 2060–2072 <https://doi.org/10.1111/jasp.12158>
- Gayle. V. (2018). Santander's fake 'money mule' job advert convinces 32 per cent of Brits to take illegal job. *Daily Gazette*. <https://www.gazette-news.co.uk/news/15816353.santanders-fake-money-mule-job-advert-convinces-32-per-cent-of-brits-to-take-illegal-job>
- Koch, T., Gerber, C., & De Klerk, J.J. (2018). The impact of social media on recruitment: Are you LinkedIn? *SA Journal of Human Resource Management/SA*. 16(0). a861. <https://doi.org/10.4102/sajhrm.v16i0.861>
- Khormi S, Ageel M, Otayf S, Al-Shafai H, Majrashi,S, & Hakami N. (2016). Addiction to Social Media among Students at Jazan University. *International Journal of Academic Scientific Research*, 4(4): 176-180.
- Latif, A. & Abdul-Rahman, A. (2018). Combating Money Laundering in Malaysia: Current Practice, Challenges and Suggestions. *Asian Journal of Accounting and Governance*. <https://doi.org/10.123-134.10.17576/AJAG-2018-10-11>
- Leukfeldt, E.R. (2014) Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime*, 17(4) 231-249. <https://doi.org/10.1007/s12117-014-9229-5>
- Leukfeldt, E. R., & Jansen, J. (2015). Cyber criminal networks and money mules: An analysis of low-tech and high-tech fraud attacks in the Netherlands. *International Journal of Cyber Criminology*, 9, 173-184. <https://doi.org/10.5281/zenodo.56210>
- Leukfeldt, E. R., & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In S. Hufnagel, & A. Moiseienko (Eds.), *Criminal Networks and Law Enforcement: Global Perspectives on Illegal Enterprise* (pp. 75-89). New York: Routledge <https://doi.org/10.4324/9781351176194-5>

- Magalla, A.B. (2018). Prevention and Detection of Cyber Crimes in Tanzania as Described by Cyber Crime Act, No. 13 of 2015. *Electronic Journal*.
<https://doi.org/10.2139/ssrn.3136637>
- Malaysia Communication and Multimedia Commission (2019). *Internet user survey 2018*.
<https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf>
- Malaysian Computer Emergency Response Team. (2019). *Reported incidents based on general incident classification Statistics*.
<https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932>
- MatIsa, Y., MohdSanusi, Z., Haniff, M.N., & Barnes, P.A (2015). Money laundering risk: From the bankers' and regulators perspectives. *Procedia Economics and Finance*, 28,7-13.
[https://doi.org/10.1016/S2212-5671\(15\)01075-8](https://doi.org/10.1016/S2212-5671(15)01075-8)
- Middlesex University. (2019). *Student fraud : Money mules*. <https://unihub.mdx.ac.uk/student-life/announcements/2019/student-fraud-money-mules>
- Muniandy, L., Muniandy, B., Samsudin, Z. (2017). Cyber Security Behavior among Higher Education Students in Malaysia. *Journal of Information Assurance & Cyber Security*, Vol 2017. <https://doi.org/10.5171/2017.800299>
- Royal Malaysia Police. (2018). *Police: Beware of mule account scam*.
<https://www.thestar.com.my/news/nation/2018/12/29/police-beware-of-mule-account-scam>
- Royal Malaysia Police. (2019). *Commercial Crime Investigation Department*.
<http://www.ccid.my>
- Shafique, F., Anwar, M., Bushra, M. (2010). Exploitation of social media among university students: a case study, *Webology*, Vol. 7, issue 2, article 79.
<http://www.webology.org/2010/v7n2/a79.html>
- Shimbun, Y. (2014). Cyber Wars/Job-seeker turned into 'money mule'. *Asia News Network*.
<https://www.asiaone.com/cyber-wars-job-seeker-turned-money-mule>
- Silverman, C. (2019). Facebook Removed Over 2 Billion Fake Accounts, But The Problem Is Getting Worse. *BuzzfeedNews*.
<https://www.buzzfeednews.com/article/craigsilverman/facebook-fake-accounts-afd>

Thomson Reuters. (2019). Revealing the true cost of financial crime:2018 survey report.

Retrieved from <http://solutions.refinitiv.com/FinancialCrimeReports>

United Nations Office on Drugs and Crime. (2019). *Money-laundering and globalization*.

<https://www.unodc.org/unodc/en/money-laundering/globalization.html>