International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 391-397

When Love is Jeopardized: Governing Online Love Scams in Malaysia

[1]Saslina Kamaruddin, [2]Wan Rosalili Wan Rosli, [3]Ahmad Ridhwan Abd Rani,
[4]Noor Zira AzlinBte Md Zaki, [5]Mohd Faizal Omar
[1]*Faculty of Management and Economics, Universiti Pendidikan Sultan Idris, 35900 Tanjung Malim, Perak, Malaysia, saslina@fpe.upsi.edu.my*
[2,3]*Faculty of Law, UiTM Shah Alam, Selangor, Malaysia, [2]rosalili@uitm.edu.my*
[4]*Faculty of Business & Information Science, UCSI University, Malaysia, zira@ucsiuniversity.edu.my*
[5]*School of Quantitative Sciences, Universiti Utara Malaysia, Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia, faizal_omar@uum.edu.my*

Abstract

In this era of globalization, the way people communicate and build relationships have evolved from the real world to cyberspace. The Internet creates opportunities for users to find romance and have affairs with people anywhere in the world. Due to this, apart from finding true love, many fall prey to the hands of scammers that aims to cheat another for money and even reputation. Last year, it was reported that more than sixty-eight million ringgit was loss due to romantic scams and the most targeted victims are lonely and elderly women. The main objective of this study the typology and the modus operandi of love scams. The paper would also analyze the existing problems in the current legal framework governing love scams and aims identify the loopholes within the current legislation in dealing with the problem. A doctrinal legal research method will be used in this article. The author contends that the scattered legal and regulatory landscape has contributed to the growing cases of love scam and thus, reform is needed to effectively govern the crime. In addition, the governance of cybersecurity can also be improved with the advancement of analytic tool to combat love scam in Malaysia.

Keywords: *Internet, Cyber Fraud, Love Scam, Governance, Malaysia.*

Introduction

The aggressive growth in technology in the past decade had greatly impacted major sectors such as information and communication technology, security, education, manufacturing and healthcare(Arora, 2016). Malaysia is at the forefront as the country is going through the process of digitalization and access to the Internet have become easier and faster which results to a significant rise in cyber activities which changes how one go about their daily lives. The phenomenal growth in the cyberworld provides new challenges to the government and also computer users in dealing with new crimes, hybrid-crimes and data-related issues (Wan Rosli, W.R, Kamaruddin, S, Hamin, Z., 2019).

The internet romance scams, Nigerian Scams or Love Scamsis a type of cyber fraud which involves romantic intentions towards the prey where the perpetrator pretend to form a relationship via online dating sites or social networking sites by gaining their trust and affection to commit fraud towards their victims (Whitty and Buchanan, 2012). Sorell and Whitty (2019) contends that online romance scams happen when these scammers defraud victims by demanding large sums of money and also would inflict serious psychological harm. San O'Key (2008) rightly argues that the fast advancement of technology enables cyber criminals to use the cloak of anonymity in cheating the victims online.Love scams would usually happen in stages and would take a few months from the beginning until the revelation of the scam(Rege. A, 2009). The main tools for the scammers are online dating sites or apps, social networking sites, and e-mail addresses to identify the victims and execute their fraudulent activities. These cyber criminals would usually identify their victims through social engineering and would usually target lone women who reach out for company or love online (Cybersecurity Malaysia, 2019). Whitty and Buchanan (2016) contends that besides the financial loss, the victims of romance scams also experienced emotional and psychological impact such as severe trauma, loss of self-esteem, depression, embarrassment, suicidal thoughts, or forced involvement in criminal activities like drug trafficking, identity theft, sexual harassment and even degradation of reputation. Similarly, O'Key (2008) highlighted that victims would usually experience emotional impact other than a pecuniary loss as a

ISSN: 2005-4238 IJAST

result of these romance scams. The US Federal Trade Commission (2019) reported that in 2018, americans have lost more than one hundred and forty three dollars to online love scams.
In Malaysia, cyber fraud is seen as a hybrid crime which is a traditional crime that has transcended into cyberspace. The surge of cybercrimes especially cyber fraud had tripled in number in the last five years (MyCERT, 2020). Yusof (2018) claims that there are 29.9 % hikes in the rate of love scams which is from 2016 to 2017, where the total amount of losses increases as 54.2 % in 2017, more than half from 2016. In general, the number of online love scams is increasing significantly in Malaysia, and have become an alarming problem that needs to be dealt with (The Star, 2019). The findings of such a report also indicate that an average of seven people isfalling victim to this love scams in a day. Also, the report indicates that the group of victims is comprised of Generation Y and Millennials and the number of victims is growing faster than expected(Vijaindren.A, 2017). The inference that can be drawn from such statistics is the exponential growth in internet romance scams over five years from 2012 to 2020. Moreover, in early 2020, MyCERT (2020) highlighted that there are more than 7,7447 cases on cyber fraud recorded and it is suggested that the actual numbers could be higher due to underreporting by victims. It was highlighted that cyber fraud which consist of romance scams are the highest type of fraud that is reported in Malaysia.
Given the issue stated above, this paper begins with the discussion on the typology and the modus operandi of love scams. The second part of this paper examines the legal position in Malaysia relating to such crime. The third part of the paper will provide the recommendation on the ways to curb love scams in Malaysia based on the analysis of the current legal position in Malaysia. The last part concludes the paper.

Typology of a Love Scam Victim

The typology of the victims of love scam ranges from the age group of around 25 to 40. Whitty (2016) contends that adults are more vulnerable compared to teenagers when it comes to love scams. Adults who have a stable job has a higher chance of becoming a love scam victim than a housewife. (Wilson, 2008).No specific gender category is more vulnerable to love scams. Both men and women can become victims of such crime.Buchanan and Whitty (2014) highlighted that victims of love scams are usually individuals who are vulnerable, romantic and lonely who are looking for companion or relationship. According to Whitty (2018) victims who are graduates and professionals can alsofall prey to love scams. The first characteristics of victims of love scams are that they are usually kind-hearted and gullible. Buchanan (2013) highlighted that victims usually trust the scammer's words whowill always use sentiments and emotions to create trust and sympathy from the victim. Research also indicates that victims are usually lonely and feels comfortable expressing themselves online and find solace in online relationships. Buchanan further contends that love scam victims will usually foster the online 'relationship' that they created as a way to get away with their loneliness (Buchanan, 2013). Next, individuals who are usually drawn to love scam will be individuals that have some romantic beliefs. Sprecher and Metts (1989) has formulated the Romantic Belief Scale where people who usually scores a high score in this test are those whole believe in destiny and that if two people are meant to be with each other, no time and place may be an obstacle. Victims usually have a strongerbelief in love and relationship to overcome their feeling ofloneliness(Buchanan, 2013).
Thirdly, love scam victims are usually sensational seekers as they are ready to take on physical, social, and financial risks just for the sake of gaining experience (Shaariet.el, 2019). According to Zuckerman (1978), there are a few factors that determine sensational seeking which is trill and adventure-seeking, experience andsexual desires. All ofthesefactors are interconnected in sensational seekers'love challenges, and they are willing to do anything for something that may as well fulfill their demands and needs. Since love scam involves a lot of emotions, victims tend to be more gullible and blind. Those who have a stronger sensational seeking desire in them are most likely to become a victim to those with lesser sensational seeking desire in them (Zuckerman, 1978). Furthermore, research found that people who are overly attached have a higher risk of becoming a victim as they tend to seek approval from the perpetrator (Tetera, 2016). They will be highly affected when scammers are mad and shows any disagreement (Tetera, 2016).

Research also indicates that there are several red flags that proves a person have been scammed. Popular reasonsused by scammersinclude sudden emergency, wanting to book a flight, family problems, medical problems,andbusiness-related problems (The Star, 2019). Scammers would also sometimes use blackmail to get what they want by using intimate pictures shared during the course of their cyber relationship. Victims often refuse to report about being scammed as they would feel ashamed and traumatize with the whole situation. Research highlights that victims would go so far as taking loans or empty their savings to help the scammers. Due to this, the impact of such crime would involve post traumatic disorder, low self-esteem, health problems, bankruptcy and even suicide (Koop, 2015).

Modus Operandi of Love Scams

Many forms of love scams had existed even before the era of the internet. One of the examples is where letters with romantic messages would be sent to the victims via post and would establish trust and also a strong romantic relationship. After establishing such trust, the scammer start asking for money from the victim (Arms, 2010). In the last two decades, after the birth of the Internet,love scams now have moved into thecyberworld. Scammers now have access to a bigger pool of potential victims that are topographically scattered without any difficulty and obscurity(Whitty,2019). In carrying out the crime, scammers canoperateindividually, in a pairs or having an organized network (Sean O'Key,2008). These scammers would usually utilize authentic dating sites as platforms for searching and identifying their prey. Initially, a fake profile which includes fake pictures is published on the website and these scammers wouldbuild and articulately create flirtatious worded exposition to lure potential victims (Evens & Petrie, 2019). The perpetrator will utilize photos that range from low-quality to intensely pixilated photos to brilliant studio shots of local or international models or army personal which reinforces the scammer's believability in supply endless photos at the victim's demand (Ghana, 2009).
The second stage includes contact. In this stage, the scammer often starts communication with the attended victim. The scammer at that point set up a solid bond with their prey through steady correspondence to create trust, and romantic contacts. This stage can last between the range of six to eight months untill the coveted trust-level is accomplished (Sean O'Key, 2008). Love scams are unbiased in gender terms which focus on males and females equally. In the third stage, the scammers would ask for cash from the victims by describing heart-breaking or urgent conditions, for example, robbery of personal documents during travel, medical expenses from sudden ailments or accidents, or financial assistance for travel to meet the victim(USDOS, 2007). Furthermore, these situations are regularly consecutive where the scammers in every case needs more monetary help as the desperate conditions heighten. The 'cycle of fraud' proceeds until the point when victims lose persistence or acknowledge they are being deceived and finally stop transferring money to the perpetrator (IC3, 2007). Given the measure of time and efforts attempted by the scammers to set the basis and trust, normally victims do not understand they are being misled or scammed(USDOS, 2007). Dixon (2005) highlighted that one of the biggest network of scammers originated from Nigeria hence the name Nigeria Scam. This network of scammers would recruit young individuals who are usually students who are good with computers and they will be sent for training on how to romance women and men (Cybersecurity 2019). The modus operandi of these scammers network would usually involve the extraction of a large number of American email addresses and sending more than five hundred fake messages every day. Different members are given different portfolio's which ranges from setting up profiles, utilizing pictures from demonstrating sites around the world, extracting or finding potential victims through social engineering or scout different platforms of social media for victims (Cybersecurity Malaysia, 2019). This comprehensiveeffortresults to the scam network getting around seven answers every day. Dixon (2005) highlighted that when an e-mail is answered by a potential victim, there is a seventy per cent chance that the scam will be successful.Nigerian scammers earned roughly $45 million consistently through these romance scams (Dixon, 2005).
On the other hand, the modus operandi of an individual scammer can be seen in a local case. An administrative associate enters into a relationship with another individual that she met online, to later discover that the "attractive American man" she met on WeChat was a con artist and blackmailer. (Loh. I, 2018) The 24-year-old, recognized just as Amy, officially paid more than RM39,000 (S$13,180) to "Morgan Deavour Andrew," whom she met in September. She said they just talked via web-based

networking media, yet she felt that they were extremely compatible and experienced passionate feelings for him. At some point, he revealed to her that he required cash for his debilitated mother's treatment and requested to acquire RM1,000 because he had lost his wallet." He advised her to bank the cash into an account in the name of NurulHekmah and continued requesting more cash after that. (Loh. I, 2018) She said she continued sending him cash and even obtained some money from her friends after spending every one of her reserve funds. Amy said "Morgan" guaranteed to come to Malaysia and reimburse her in full, however on Jan 18, he revealed to her he had been kept at Kuala Lumpur Worldwide Air terminal and required more cash for his discharge. She just acknowledged that she was being duped. When she declined to send him cash, he debilitated the authorities would discover and uncover her nude pictures in his bags at the Airport. Amy said he kept on annoying her, yet she quit conversing with him (Loh. I, 2018). Little-scale scam organizations with comparative objectives can coordinate effortlessly and with speed. These criminal associations frequently utilize love scams as a forerunner to different crimes, for example, reshipping stolen merchandise, money related extortion, and personality misrepresentation (Bossler et. al, 2019).

The Laws Regulating Love Scams in Malaysia

Online love scam is a type of crime or fraud that can be governed under the Penal Code. Based on the Penal Code, the crime of online romance scams may be covered by the provisions under section 415 until section 420. Section 415 provides the provision for cheating, and section 416 governs the crime of cheating by personation. The perpetrator who commit crimes under sections 415 and 416 can be punished with fine or imprisonment for five years and with seven years of imprisonment or fine respectively according to sections 417 and 419. Section 420 governs aggravated cheating which involves dishonestly inducing the victimto deliverproperty andmay be applied in the circumstances where the scammers' goal is to obtain money from the victims by handing over or transferring the cash to his fellow member of the gang or partner. The elements of section 420 under dishonest cheating would involve the act of the accuse cheating the victim. Due to the accused' act or behavior, the victim is then induced to deliver property to anyone or to make, alter or destroy valuable security. The keyword or the most important element under this section is the presence of dishonest intention. in the case on Liew Min Poh v PP (1962), the prosecution must rove that there is an element of deception present during the act of cheating or fraud. The accused must have been deceived and the accused have obtained the goods through dishonest means. Dishonest intention must also be shown to exist at the time of the crime as held in the case of Yong Yong Peng v PP (1947). The judge held that there must be evidence that the accused had dishonest intention at the time of obtaining the money or property from the victim. In PP v Siti Latifah Mohd Said (2016)Latifah, 29, a part time computer application engineer was accused of masquerading as khalisyanajwa in social media and deceiving a 28-year-old man (doctor at Melaka Hospital) until the victim handed over RM75,750 (for their marriage scam) in different locations in Ayer Keroh. She was charge under section 420. The court held that the accused was gulty and she was given 21-year imprisonment and RM10,000 fine (7 charges). In PP v Mazrin Abd Aziz (2015), Mazrin, 39, an unemployed, was accused of cheating a teacher and his wife in relation to the sale of a house which was not his property at a price of RM280,000.00 at Mudah.my in 2014. The court held that he was guilty under sec 420. In another case, PP v IrwanSamsu, the accused stole the victim's ATM card and fraudulently withdraw the victim's money amounting to RM12,800 without her knowledge. The accused obtained the pin number of the ATM after telling the victim that he needed the pin number for a police investigation. The accused was founfgulty for dishonest cheating under section 420.
The crime under this section is punishable with imprisonment for ten years and also fine(Shuan. S. L. H, 2010). In Malaysia, there are several laws that could govern cybercrimes such as the Communication and Multimedia Act 1998, Computer Crimes Act 1997 and Digital Signature Act 1997. However, these laws only govern unauthorized access and also content related issues or data protection. There is no specific cyber related law which can be used to govern cyber fraud. However, since cyber fraud is not a new crime, but a traditional crime which has transcended into cyberspace, the Penal Code would be sufficient to govern such crime effectively. However, there may be challenges in terms of evidence or investigation as love scams or cyber fraud would involve digital evidence (Kuppusamy. M and Santhapparaj. A. S, 2006).

In the case of Pp v jamaliah Abd Rahman (2016), the accused cheated the victim who is a medical doctor stating that she could arrange for the saleof several luxury cars which the Attorney General's Office needs to sell off. The accused stated that she could get a car for the victim. In lieu of that, the victim paid the accused in stages from 2001 to 2003 amounting to RM257 308. The accused also impersonated the AG by SMS to the victim in order to induce him to deposit RM34 500 into two bank accounts in 2005 as stamp duties to take out the alleged cars. The accused was finally charged and pleaded guilty for dishonest cheating under section 420 and also cheating by impersonation under section 419 of the Penal Code. The accused was sentenced to six years of jail for the first offence and two years' imprisonment for the second offence.

In an unreported case, a love scam victim that have lost more than one million dollars. It started when the victim, Mary, accepted a friend request on Facebook. The scammer who claimed that he was an American engineer and investor have scammed 1.2 million dollars from her. Being convinced that he was in love with her, Mary who craved companionship at the moment have accepted him with open arms. She claimed that her husband has no time for her and all the children are grown-ups. It all began when the scammer asked her to look for a place to rent nearby where she lived. He began by asking her help to deposit the 6000 dollars for the house deposit and then told her that he was stuck in the airport for bringing so much cash. He then asked her to help pay 50 000 dollars first, and he promised to give back the cash to her once they meet. Mary agreed to do so as she was blindly in love. She was even ready to let go of her relationship with her husband for the sake of him. She even took out all her savings and insurance money. He then went missing, and he was nowhere to be found. By the time she realized she was scammed, she has lost 1.2 million dollars off her savings (Nabilah, 2016).

Potential Tools for Love Scam Detection

Artificial Intelligence (AI) is an area of computer science which refers to the computer program that mimic human intelligence or the environment. The advances of device and technology has enable more intelligence algorithm to be developed to cater complex problem. Machine Learning is one of the popular technique in AI that provides algorithms to automatically learn and experience similar to human intelligence and it is inspired by the biological human neurons. The main aim of machine learning is to allow the algorithm to learn the data and action to be taken automatically without human intervention. The main tasks of machine learning for data analysis consist of prediction and classification of data. The real world applications includes product recommendation, face detection, image recognition, fraud detection, email and malware filtering, etc.Till date, limited study has been conducted for love scam using AI tool. It is important to analyzed whether the notions of romance introduce traits that could be used to build a detection system. Tangil, Edwards, Peersman, Stringhini, Rashid and Whitty (2019), recently proposed the use of Machine Learning for early detection of love scam on online dating system. By detecting the fraudulent profiles, the machine learning algorithm is develop and compare its accuracy with a moderator. The result yield high precision of online dating fraud profiles. Figure 1 illustrates the framework of fraud dating profile detection (Tangil et al. ,2019)

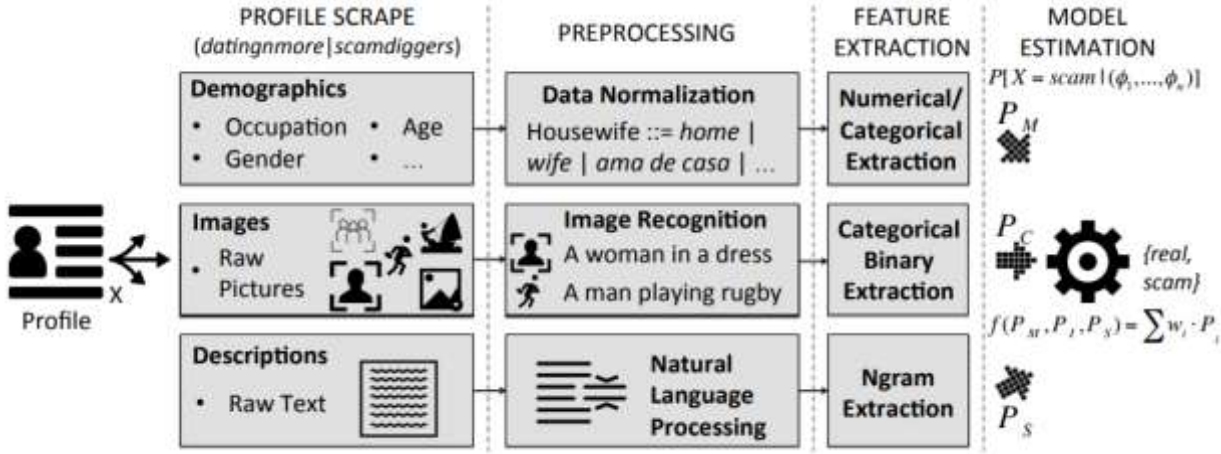

Figure 1. Fraudulent profile detection framework (Tangil et al. ,2019)

The process starts with profile scraper from online dating platforms. Image and text will be extracted. AI techniques such as Image Recognition and Natural Language Processing are used in the pre-processing stage before it is reverted to machine learning algorithm to detect the suspicious profile and compare with the targeted output.
The above preliminary work shows that AI has abundant potential for keeping people safe from internet-based scams.The approach used to overcome the love scam problem will evolve and will get more advanced as time goes by. In Malaysia, the technology is still considerably new and more efforts are needed to safeguard the internet user from fraudulent and scam activity.

Conclusion

Taking everything into account, Malaysia has been making dynamic strides to make a safe digital platform while introducing cyber laws that may protect the interest of the love scam victims. However, in all actuality, in this constantly developing time, the digital world requires a tenacious evaluation of new digital law. Since the romance scam is a borderless offense, legislation must be transformed. Citizens should be more aware,and romance scam victims should help to create awareness among others with this issue. The parties concerned should consider this matter seriously by considering approaches to break the digital hindrance and not simply accuse the injured individual of the entirety. It does not simply concern the cash gone; it might likewise hurt them mentally. It is vital for us to recognize this problem. The government should make proactive strides in overhauling digital law and, if conceivable, have a particular law for love scams. The lesson from the US could be adopted by the Malaysian government to counter and eradicate this problem effectively.

References

1. Arms, S. (2010). Romance Scam: Scammers Feign Affection to Commit Fraud — retrieved April 2019.
2. Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviors. Perspectives in Science, 8, 540-542.
3. Azzam, A. (2014). The jurisdiction in Cybercrimes: A Comparative Study. Journal of Law, Policy And Globalization, 22(2)
4. Brenner, S. W. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. North Carolina Journal of Law & Technology, 4(1),
5. Buchanan, T, & Monica T. (2013). The online dating romance scam: causes and consequences of victimhood. doi: http://dx.doi.org/10.1080/1068316X.2013.772180
6. Charles, A. (2018). The Privacy, Data Protection and Cybersecurity Law Review. Retrieved from https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151376/united-states
7. Dixon, R. (2005). Nigerian Cyber Scammers. Retrieved April 5, 2009, from http://www.latimes.com/technology/la-fgscammers20oct20,0, 301315.story?page=1&coll=la-tot-promo
8. Hamsi, A. S., Bahry, F. D. S., Tobi, S. N. M., &Masrom, M. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. Journal of Management Research, 7(2), 169-181.
9. IC3 (Internet Crime Complaint Center) (2007). 2007 Internet Crime Report. Retrieved April 1, 2009, from http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf
10. Jurkowski., S. (2017). Computer and Internet Fraud. Retrieved from https://www.law.cornell.edu/wex/computer_and_internet_fraud
11. Loh, I. (2018, January 29). Woman 'stripped' of RM39,000 in the scam. Retrieved November 08, 2018, from https://www.thestar.com.my/news/nation/2018/01/29/woman-stripped-of-rm39000-in-scam-online-casanova-threatened-to-expose-her-nude-pictures-after-she-c/
12. Manap, N. A., &Taji, H. (2012). Cyber Crimes: Lessons from the Legal Position of Malaysia and Iran. International Journal of Information and Electronics Engineering, 2(3), 404.

13. Mohamed, D. (2012). Investigating Cybercrimes Under The Malaysian Cyber Laws And The Criminal Procedure Code: Issues And Challenges. Malaysian Law Journal Articles. 6MLJi.
14. Nawawi, M. H. (2013). SkripCintaAwalHitam. Harian Metro. 14th December 2013.
15. Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. International Journal of Cyber Criminology, 3(2).
16. Robert, J. (2012). Cooking Up a Recipe for Self-Control: The Three Ingredients of Self-Control and its Impact on Impulse Buying. Journal of Marketing Theory and Practice, 20(2). doi: https://doi.org/10.2753/MTP1069-6679200204
17. Safwan, A. (2015). Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors, and Keys to the Problem. Journal of Management Research, 7(2).
18. Shuan, S. L. H. (2010). White-Collar Crime in Malaysia.
19. Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically Dismantling Online Dating Fraud. Retrieved from https://arxiv.org/pdf/1905.12593.pdf
20. Tetera, K. (2016). These Personality Traits Make You Most Vulnerable to Online Dating Scams, Study Finds. Retrieved from http://thescienceexplorer.com/technology/these-personality-traits-make-you-most-vulnerable-online-dating-scams-study-finds
21. Whitty, M. (2018). Do You Love Me? Psychological Characteristics of Romance Scam Victims. Cyberpsychology, Behavior, And Social Networking, 21(2), 105-109. doi: 10.1089/cyber.2016.0729
22. Williams, E. (2017). Computers in Human Behaviour (72nd ed., pp. 412-421). England: The University of the West of England (UWE).
23. Wilson, A. (2008). The Effects of Loneliness on Telemarketing Fraud Vulnerability Among Older Adults. Journal of Elder Abuse & Neglect, 20(1), 63-85. doi: http://dx.doi.org/10.1300/J084v20n01_04
24. Yusof, Z. M. (2018, February 04). Online love scam victims lost record $37m in 2017. Retrieved November 05, 2018, from https://www.straitstimes.com/singapore/courts-crime/online-love-scam-victims-lost-record-37m-last-year
25. Zuckerman, M. (1978). Sensation Seeking in England and America: Cross-cultural, Age, and Sex Comparisons. Journal of Consulting and Clinical Psychology, 46(1).
26. Sorell, T., Whitty, M. Online romance scams and victimhood. *Secur J* **32,** 342–361 (2019). https://doi.org/10.1057/s41284-019-00166-
27. Karimi, F. (August 23, 2019). Americans lost $143 million in online romance scams last year. That's way more than any other reported fraud. CNN news at.whttps://edition.cnn.com/2019/08/23/us/online-romance-scams-losses-trnd/index.html
28. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*.
29. Petrie, E., & Evans, C. (2019). Piloting the Exchange of Insider Threat Reports: Information Sharing Challenges to Proactive Cyber Fraud Identification.
30. Bossler, A. M., Holt, T. J., Cross, C., &Burruss, G. W. (2019). Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*, 1-18.