Pakistan Journal of Criminology
Vol. 15, No. 04, October-December 2023 (667-681)

Cybercrime in Malaysia - Prevention of Honey Trap on Social Media and Online Dating Applications

Norazida Mohamed [1], Nasir Sultan[2],
Vivien NG Wai Yan[3] & Siti Jalilah Mat Husin4[4]

Abstract

The study explores the weaknesses of the internal control mechanism of dating applications and social media platforms to prevent innocent users from fraudsters. The study applied a qualitative technique and adopted the semi-structured interviews method to achieve the study objectives. The semi-structured interviews were conducted to gain first-hand information concerning love scams. The study found that most dating applications have feeble internal control mechanisms concerning registration. Therefore, fraudsters can trace and approach potential victims easily. For the prevention of users from scammers, the identification process should be strengthened by introducing stringent identity requirements.

Keywords: Cyber scams, Preventive measures, online love scams

Introduction

A divorcee from Chicago became a victim of a scam by a man she met online. A fraudster manipulated her, causing her to lose her savings, half of her retirement money, and the proceeds from two loans she took out for him (Weisbaum, 2020). In another case, a Malaysian Widow lost RM1.15 million to a man she met through a chat and dating application (Singh, 2020). Such incidents are happening globally, and their frequency is increasing extraordinarily. These incidents have serious economic and psychological consequences. Therefore, it is important to study preventive measures against these disturbing crimes.

Digital development has brought substantial changes into our lives. We witness the unprecedented transformation from analogue to digital, and it's still going on. It has indeed transformed the lives of many in developing and developed countries (Aly, 2020). For example, three decades ago, long-distance communications were mainly via postal services or telephone. Now, most of the world is connected via digital networks that enable enormous volumes of text, images, audio, and videos to be exchanged in real time (Cruz-Jesus et al., 2016).

[1] The author served as an associate professor at the Accounting Research Institute, University Teknologi Mara (UiTM), Shah Alam, Malaysia. Azida767@uitm.edu
[2] The author is the correspondence author and assistant professor at the Department of Management Sciences. University of Gujrat, Pakistan. Nasir.tarar@uog.edu.pk
[3] She is associated with Help University, Malaysia.
[4] The author is associated with the Accounting Research Institute, University Teknologi Mara (UiTM), Shah Alam, Malaysia. jalilahwork@gmail.com

However, these developments bring new fraud techniques, like cyber love scams (LS). However, prevention measures are not developed accordingly.

Over half of the world uses social media platforms (Kemp, 2020). There are various social media platforms, such as Facebook, Instagram, WeChat, and Twitter. These platforms instantly became the primary way of communicating and socializing globally, especially during COVID-19 (Seal, 2020). Social media platforms have become affordable and convenient (Cuncic, 2019), thus providing abundant opportunities to interact with new people (Lenhart, 2015). Dating has also gone virtual, and dating applications are providing opportunities to meet potential partners, without providing proper safety measures.

Therefore, online dating websites and applications are becoming an increasingly accepted way to meet a potential partner (Stoicescu, 2019). For example, it enhanced web-based courtship across the US and Canada (Rose, 2012). Three in ten Americans used an online dating site or application to find a match (Anderson, Vogels, and Turner, 2020). The ratio in other parts has also increased, especially during COVID-19, which limits the physical contact of people. There is an 82% increase in dating application usage (Dating.com, 2020). The ratio has also increased in Malaysia, as 29 percent of the population uses online dating applications (YouGov, (2017). Incontrast preventive measures were not advertised and adopted by regulating agencies and by public at at large.

However, despite all security measures by social media operators, the risk of cybercrime is unavoidable. Cybercrime has emerged as a major concern for both corporations and individuals. The global annual cybercrime cost was $3 trillion in 2015, predicted to grow to $6 trillion annually by 2021 (Morgan, 2016). The cost is made up of losses from cybercrimes such as damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm (Cruz-Jesus et al., 2016).

Federal Trade Commission received 25,000 complaints on online romance fraud and a loss of $201 million (Span, 2020). The love scam cases increased by 40 percent in the US during COVID-19 (Stewart, 2020). In Malaysia, 1,652 love scam cases involving RM61.9 million in losses were reported in 2017, and 1,301 cases with losses amounting to RM83.6 million between January and August 2018 (Bahaudin, 2018). Royal Malaysian Police (RMP) has recorded 4,673 love scam cases that were reported between 2013 and May 2016, involving losses amounting to RM182.3 million (Zahid, 2016). It has illustrated that love scams are occurring commonly in Malaysia.

Malaysia Commercial Crime Investigation Department opened 11,875 cybercrime investigation papers in 2019, compared to 10,753 in 2018. The economic loss increased by 24.9 percent, reaching RM497.7 million in 2019 from RM398.6 million in 2018 (Malay Mail, 2020). Malaysian's spending on dating applications in 2019 amounted to RM24 million, approximately twice in 2018 (Shaari, 2019). Malaysia's overall IT spending reached to staggering $ 11 billion (Yap, 2020). Digital transformation is accelerating in Southeast Asia, and it is expected that by 2021, at least 48% of the region's GDP will be derived from digital products and services (Yap, 2020).

Previous studies were primarily focused on the psychological effects on victims like Coluccia et al. (2020), Whitty (2018), Whitty and Buchanan (2016), and Whitty and Buchanan (2012. Several other studies discussed the modus operandi of love scams, i.e., Whitty (2015), Shaari et al. (2019), and Kamaruddin et al. (2020). Nonetheless, rare studies discussed the prevention measures implemented to deter the possibility of love scams. Therefore, this study explores love scams' motives and how to prevent potential victims from cyber love scams through dating/social media applications.

Literature Review

The internet has radically changed how people work, socialize, create, and share information, ideas, and things globally (Manyika & Roxburgh, 2011). Therefore, the world is becoming more connected through various digital developments. It has given people more opportunities to initiate contact with potential romantic or sexual partners (Sumter & Vandenbosch, 2019). These developments influence young adults much more than others, as a significant percentage between 18-24 use online dating services (Flug, 2016), as initiating a committed relationship has become one of the primary goals of people in their young adulthood (Goldmann, 2020).

Cybercrime is sometimes known as cyber fraud (Goldmann, 2020) or cyber scams (Bernama, 2019). Such scams are rising around the world as the technology inventions progress. Some notable cybercrime includes email and internet fraud, identity fraud, theft and sales of corporate data theft, financial or card payment data theft, cyber extortion, ransomware attack, crypto-jacking, and cyber espionage (Kaspersky, u.d.). Online love scams are another serious cybercrime (Whitty and Buchanan, 2012).

Love scams are also known as romance scams (Whitty, 2015; Stewart,2020) or romance fraud (Span, 2020). It happens when the scammer assumes a fake online identity to gain affection and trust from the victim and uses the illusion of a romantic or close relationship to manipulate the victim (Stewart, 2020). Therefore, a love scam

is a relationship created through the internet's facilitation on the world wide web to deceive unsuspecting victims to extort money from them (Whitty, 2013). Further, love scams emerged as mass-marketing fraud (MMF), which abuse mass communication techniques such as email, Instant Messenger, bulk mailing, and social networking sites to deceive people for money Whitty (2018).

Online dating is made possible through social media platforms such as 'Facebook' and 'WeChat,' as well as through dating applications such as 'Tinder' and 'Coffee Meets Bagel.' Dating applications are software applications designed to generate connections between people interested in romance, casual sex, or friendship (Orchard, 2019; Sanders, 2011). These platforms are safe to be used to connect people around the world. Therefore, social media has become a place for people to meet easily, socialize and become acquainted online (Izang et al., 2019). However, not everyone is using these platforms judiciously. Therefore, these platforms are providing opportunities to cybercriminals, including love scammers (Whitty, 2017).

A love scam takes place as the fraudster creates a fictitious profile on the platforms to lure potential victims into the scam (Saad, Abdullah, and Murah, 2018). The fraudsters exploit common interests and use persuasive language to manipulate victims (Sharri et al., 2019). Later, scammers trick victims by demanding large sums of money while inflicting severe psychological harm (Sorell and Whitty, 2019). Women turned out to be easy prey to scammers despite exposure and various awareness campaigns. Most victims of love scams fall in the age group of 25-40 years (New Straits Times, 2018). Furthermore, perpetrators use online dating sites or applications and social networking sites as the main tools to identify the victims and execute their fraudulent activities (Kamaruddin et al., 2020).

Victims who have gone through love scams would suffer from several impacts. Generally, the effects can be categorized into financial and psychological (Whitty and Buchanan, 2015). Losses from love scams amounted to $83 million in 2019, up from $60.5 million in 2018 (Cross, 2020). On the other hand, Malaysia has also reported 1,652 cases of love scams amounting to RM61.9 million in 2017 and 1,301 cases with losses involving RM83.6 million in the first eight months of 2020. The psychological impacts are considered more severe than economic losses (Whitty and Buchanan, 2015).

The main psychological effects include depression, shame, embarrassment, shock, anger, guilt, and fear (Whitty and Buchanan, 2015). Psychologically, the victims have high levels of neuroticism, sensation seeking, impulsiveness, and dependency (Coluccia et al., 2020; Whitty, 2012; Whitty and Buchanan, 2014). Further, victims also lack self-control, possess characteristics of addictiveness, are highly educated, and are less kind (Whitty, 2017). Furthermore, lonely individuals

seeking companionship tend to be more susceptible to love scams. Therefore, middle-aged single women are considered more prone to LS than men (Whitty, 2017).

The occurrence of a love scam can be explained using Routine Activity Theory by Felson and Cohen (1974). According to the theory, there are three necessary conditions for crimes to occur: a likely offender, a suitable target, and the absence of a capable guardian. In a love scam, the likely offender is a fraudster who creates a fake online identity to gain affection and trust from the victim and uses the illusion of a romantic or close relationship to manipulate or steal from the victim (Stewart, 2020) on dating applications and social media platforms. These fraudsters are using the platforms intending to defraud the victims of their money. For Example, a victim of a love scam loses RM10,400 (Astro, 2020); in another case, a single mother lost more than RM480,000 to a love scam (MalayMail, 2020). According to the routine activity theory, these fraudsters and love syndicates represented the likely offender.

Lastly, the absence of a guardian, as stated by the routine activity theory, also contributes to crime. In a love scam, the loophole in the internal control mechanism has made the scam possible. It is because of the lack of internal control mechanisms that creating fake profiles on these platforms is possible. In the studies by Kamaruddin et al. (2020), Buchanan and Whitty (2013), Whitty (2012), SundayPost (2020), and NBCNews (2020), the love scam incidents that were studied and reported revolves around fraudster who created fake profiles on the platform before they use these fake profiles to approach the victims. The possibility of creating fake profiles happens because there is an absence of guarding to review these profiles for prevention of fake profiles that fraudsters could use to commit love scams against the victims.

The consequences of fake love scams include physical harm to victims, mental torture, and financial loss. Several innocent people were trapped in LS mainly due to poor monitoring and technical loopholes in social media platforms. Moreover, it is equally important to understand why a particular age group is more vulnerable to LS and what type of people become easy prey to criminals. Therefore, keeping LS's intensity, gravity, and volume is paramount to developing and implementing robust regulations against such cybercrimes. Thus, this study focuses on the Cyber love scams in the Malaysian context.

Research Methodology

This research adopts a qualitative approach. The qualitative approach is the systematic inquiry into social phenomena in natural settings (Teherani et al., 2015). As this research covers the study of the environment of social media platforms and dating applications, the use of a qualitative approach will be the most appropriate.

This research explored the vulnerabilities of love scam victims and what preventive measures can be implemented to reduce the occurrence of love scams. Adopting the ethnography, researchers will learn the hands-on experience of using the platform as a use.

A semi-structured interview was developed for this study. Through the interview, researchers are able to explore the understandings, experiences, opinions, and motivations of individuals on a particular concern (Gill et al., 2008). The interviews with enforcement officers helped in obtaining first-hand information concerning the common tactics and modus operandi of perpetrators. It ultimately leads to identifying weaknesses in the existing system. Information on victims' psychological and demographical traits is also obtained for the analysis on its relationship with the vulnerability of victims towards love scams to satisfy the study's objectives. As the information is received, it acts as a vital point to prove the importance of preventive measures, as the information on the economic losses data is also obtained from the targeted respondent for the analysis. This information obtained is linked to each other to show the relationships between the vulnerability of victims and the economic losses from the scam, indicating that the impact of the scam is alerting.

A few interviews were conducted with the Head of the Malaysia Cyber Emergency Response Team (MyCERT) and the Senior Vice President of Cybersecurity Malaysia. MyCERT, operating under CyberSecurity, provides a platform known as Cyber999 to the general public to lodge reports related to cyber incidents, which will be categorized into nine categories, including cyber fraud. Besides, CyberSecurity also acts as a digital forensic for law enforcement agencies in providing cybersecurity-related technical assistance and advice for the investigation of cyber-related cases. In the interview, a list of questions was asked to identify the traits of victims and the modus operandi of instrumenting the scams. Besides, the number of love scam cases which was reported in Kuala Lumpur was also obtained to ascertain if, in personal view, is the scam deemed to be significant and alerting.

Research Findings

The study has selected four platforms for the registration process: Facebook, WeChat, Tinder, and CoffeeMeetsBagel ("CMB"). The researcher has tested the registration controls on all these platforms by registering a new account on all the selected platforms.

A. Registration process of platform

It was found that among the selected platforms, Tinder's registration process has minor requirements before enabling the user to use the account to meet other users on the platform. In the Tinder registration process, the user must verify the mobile number. The mobile number is the username to log into the account. After the verification of the mobile phone using a One Time Pin ("OTP") received through short message services ("SMS"), the user is required to enter the email address to secure the account. However, the account can still be used without any verification. In setting up the user profile, the user needs to upload two photos and other basic personal information such as display name, birthday, and passion. However, it does not require the user to upload a photo showing the user's face. Although there is a verification feature in the application that requires users to take selfies to verify against the photo uploaded, it is not a requirement to enable users to use the platform.

In the CMB application, the registration process is similar to Tinder, which requires the verification of a mobile number by receiving an OTP through SMS. However, CMB does not require the verification of email addresses, although it is needed as personal information for CMB to deliver marketing materials. The profile setup also requires personal information such as display name, birthday, gender, and type of relationship that the user is looking for. In addition, CMB requires a clear photo showing the user's face before approval of the accounts. Without the approval, CMB will not show the profile to other users. Nonetheless, it was noted in the study that any photo without a covered face will enable the account to be approved regardless of whether the person in the picture is the actual user.

On Facebook, the registration process only requires an email address as an account username. The registration details need basic personal information such as name, date of birth, and gender. Facebook also requires a verification of email address. The user would receive a code through email that needs to be keyed into Facebook as a verification procedure. Unlike CMB and Tinder, Facebook's registration process does not require users to upload photos before accessing and using the platform to create relationships with other users of the platform.

On WeChat, the registration process requires the use of a mobile number as the username to sign up and log in to the platform. The registration process requires basic information such as name to sign up. After the information is provided, the platform will require a verification of the mobile number through OTP via SMS. In addition, WeChat also requires an existing user to verify the new user by scanning a QR code of the new user before approving the account to be used by the user. WeChat also sets a limit on how many users an existing user can verify within a stipulated timeframe. Similar to Facebook, WeChat does not require users to upload any photos of users before accessing and using the platform to connect with other users.

B. Awareness campaigns and information on the platform

Table 1: Availability of Safety Information

Platform	Prompting of awareness information/ message	Availability of information/ message on the safety of usage	Cover on connecting with other users
Tinder	No	Yes	Yes
CMB	Yes	Yes	Yes
Facebook	No	Yes	Yes
WeChat	No	Yes	No

During the usage of Tinder, there are no awareness campaigns, and information on the safety usage of the platform is shown to the user of the platform when the user is "swiping" on the user profile to get a match. However, there is information on safety tips and community guidelines for users to read through. To access these guidelines and recommendations, the user must click on the settings tab and scroll to the bottom. In the safety tips section, there is information on online safety regarding financial information, personal information, and warning towards users to keep conversation in the platform as Tinder has implemented a Safe Message Filter to detect users with bad intentions. This section also advises users to be cautious of long distance and overseas relationships as it is a common red flag of scammers. Tinder also provides safety cautious that can be taken by users when meeting with other users in person as well as sexual health and consent-related matters. In addition, Tinder also provides community guidelines on what is allowed and disallowed on the platform. If users notice other users fail to adhere to these guidelines, they can report the relevant profile to Tinder for further action.

On the CMB platforms, a constant reminder is shown to users who do not upload a clear photo of the user that the user profile will not be approved to be shown to another user on the platform regardless of whether the user "swipes" on another user profile. Besides, CMB also has information on safety, security, and privacy for users to read through. To access this information, the user will need to go to the profile tab and then select "Help & Support." In the "Help & Support" section, the "Safety, Security, and Privacy" section is accessible. In the section, users can search for topics they would like to read about. In terms of the safety of platform

usage, there is a highlighted section that provides tips to stay safe while looking for a potential partner on the platform. However, users must search separately with relevant keywords for other safety tips and community guidelines. These safety tips and community guidelines include spotting a scammer and reporting other users on the platform.

On Facebook, there is no awareness message or information prompt for users to be aware of the risks of using the platform to meet people. To access the privacy and security guidelines, users must click on the user menu and then click on "Help & Support" to access the "Help Centre." In the Help Centre, users can access the "Privacy and Security" section. The guidelines and information contain information on how to stay safe on the platform. However, these guideline does not specifically contain information on meeting people. Still, it only covers abuse resources, suicide and self-injury resources, crisis response, safety resources for parents, and info for law enforcement. It also has a guideline on reporting anything that goes against the Facebook Community Standards to the administrator for action to be taken. The Facebook Community Standards cover the authenticity of users, safety, privacy, and dignity of people.

On WeChat, there is no awareness message or information prompt for users to be aware of the risks of using the platform to meet people. The platform also does not have any guidelines or safety tips aimed at people who use the platform to meet new people through the feature of "Shake" or "People Nearby." Although there is a "Help & Feedback" section, which can be accessed by clicking on the "setting" tab, the information in the section is only on account maintenance rather than community standards or user safety.

C. Traits of victims and modus operandi

With the data collected from CyberSecurity through the interview, victims of love scams were mainly female, within the age group of 18 – 45 years old. Regarding psychological traits, the victims are primarily lonely and desperate for companionship and attention. These traits were mainly the root cause of the victims who fell prey to the scam, as fraudsters took this as an opportunity to entice the victims to obtain economic gains.

The modus operandi used by the fraudsters to instrument the scams is generally the same regardless of the background or traits of the victims, as organized crime groups trained the fraudsters to commit such fraud. The fraudster would start by assuming fake profiles on social media and dating applications, equipped with fake pictures that posed them as a good-looking or wealthy person, to identify the potential victims. The fraudster will then approach all possible platform users and tag anyone responding to their scheme as their prey. The fraudster uses

well-fabricated fake profiles when coming to the victims to make them feel that they are fortunate to meet someone with a good background.

Once the victim is identified, the fraudster would use sweet words and promises when socializing with the victims, such as praising the victims, enticing the victims with love and passionate words with promise to become the victims' love partner to lure the victim into the scam through the making the victims feel affectionate and loved. Once the fraudster gains the victim's trust, they will start to request money for various reasons or request the victim to purchase valuable items to be delivered to them. This modus operandi was also used by the fraudster in many cases reported in the news report, which includes reports by Tan (2019), and Utusan (2018).

D. Existing Preventive Measures

Current preventive measures are mainly of awareness in nature. It can be seen from the awareness message and information that is provided by the platform. Besides, supporting agencies such as CyberSecurity Malaysia also conduct awareness campaigns through CyberSafe to highlight the issue of love scams through media and education to the general public, children, and adults, and to provide knowledge and best practices on the internet to protect against cyber threats, including love scams. In addition, CyberSafe also conducts awareness programs such as talks and seminars in educational institutions to highlight the concerns on cyber threats and methods to protect against such threats.

Data collected through observations and testing of the selected platforms suggested that the registration process contains weaknesses. A common imperfection noted is that these platforms do not require genuine identity verification before enrollment into the platform. Although there were mechanisms to verify through email address or mobile phone number, email and mobile phone number itself can easily be obtained without proper verification in the first place. This leads to the fact that email address and mobile phone number verification is not a strong control mechanism.

Furthermore, not all platforms require profile photo verification to ensure the user is not creating a fake. Although there are image recognition measures in CMB, an enhancement compared to the other platforms, it could not constitute an effective mechanism as well due to the platform allowing uploading of any photo that shows a clear face and not necessarily a picture of the user. Similarly, the 'existing user verification' process in WeChat may not be an effective way to deter abuse of the platform, as the older WeChat account may still be fake. From the modus operandi that is seen and reportedly used by the fraudster, this mechanism weakness is the source of a loophole that has provided an opportunity for the fraudster to pose with a

fake profile on the platform in the hope of tricking another user into falling prey into the love scam.

With love scam cases being raised, it has become a significant concern. The study suggested that the existing prevention measures, which focus mainly on awareness, are not effective in preventing the victim from falling prey to scams that are instrumented by the fraudster. Although an awareness campaign has been carried out to enforce the awareness message toward the general public, the losses from love scams are still significant, with cases where losses suffered as much as RM 480,000 (Bernama, 2020).

The finding also demonstrates that the delivery of awareness campaigns or cautious information available on the tested platform is not effective and efficient in all tested platforms, especially on WeChat, as it is not accessible on the platform. For the other three platforms, this information requires multiple steps to be accessed, which is not very user-friendly as it requires extensive steps prior to arriving at the destination page, except CMB, where prompting of notification for photo verification is available.

Conclusion and Recommendations

The study concluded that the feeble control mechanism of the registration process on social media and dating applications poses a significant risk to potential victims. It provides opportunities for fraudsters to identify, track, develop relationships, manipulate, and hunt down the victims economically and psychologically. The criminals frequently practice fake identities to defraud victims. However, the internal control mechanism is feeble in most social media platforms. To protect and prevent the masses from such scams, stakeholders must focus on awareness programs. However, these programs are less effective because they are insufficient. Therefore, the platform may implement an identity verification procedure similar to an e-wallet such as Grab, a Crowd Advertising platform such as MyBump, or a foreign exchange platform such as XM.com. They require verification through a personal identity document such as an Identity Card (IC) supported with a selfie photo or proof of residency such as utility bills to ensure that the user is indeed genuine. Furthermore, the awareness information can be displayed on the interface, which requires less navigation or through notification pop-ups of such information to improve the delivery efficiency of the awareness message and information.

Acknowledgement and Funding

We would like to thank the Accounting Research Institute, UiTM, a HICoE Ministry of Higher Education for the research funding.

References

Aly, H. (2020). Digital transformation, development and productivity in developing countries: is artificial intelligence a curse or a blessing?. *Review of Economics and Political Science*, *7*(4), 238-256.

Anderson, M., Vogels, E. & Turner, E., 2020. *The Virtues and Downsides of Online Dating*, Pew Research Center: Internet, Science & Tech. United States of America. Retrieved from https://policycommons.net/artifacts/616387/the-virtues-and-downsides-of-online-dating/1597009/ on 18 Nov 2023. CID: 20.500.12592/q2dgn9.

Astro, (2020). Single mother loses RM480,000 in love scam. Astroawani. Retrieved from https://www.astroawani.com/berita-malaysia/single-mother-losesrm480000-in-love-scam-262981.

Bahaudin, N. (2018). People still falling victim to love scam despite awareness campaign. New Straits Times. Retrieved from https://www.nst.com.my/news/crimecourts/2018/09/411233/people-still-falling-victim-love-scam-despite-awareness-campaign.

Bernama. (2019). Cyber scams top the list every year. New Straits Times. Retrieved from https://www.nst.com.my/news/nation/2019/08/512452/cyber-scams-top-list-every-year

Breheny, M., & Stephens, C. (2015). Approaches to narrative analysis: Using personal, dialogical and social stories to promote peace. In *Methodologies in peace psychology: Peace research by peaceful means* (pp. 275-291). Cham: Springer International Publishing.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical practice and epidemiology in mental health: CP & EMH*, *16*, 24.

Cross, C. (2020). $2.5 billion lost over a decade: 'Nigerian princes' lose their sheen, but scams are on the rise. Retrieved from https://theconversation.com/2-5-billion-lostover-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289.

Cruz-Jesus, F., Oliveira, T., Bacao, F., & Irani, Z. (2017). Assessing the pattern between economic and digital development of countries. *Information Systems Frontiers*, *19*, 835-854.

Flug, K. C. (2016). Swipe, right? young people and online dating in the digital age. University of St. Thomas, Minnesota.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, *204*(6), 291-295.

Goldmann, P. (2020). An Introduction to Cyber Fraud. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119205654.app3

Izang, A. A., Kasali, F. A., Ajayi, W. S., & Adegbenjo, A. (2016). The role of social media on online dating and sustainable marriage.

Kamaruddin, S., Wan Rosli, W. R., Abd Rani, A. R., Md Zaki, N. Z. A., & Omar, M. F. (2020). When love is jeopardized: Governing online love scams in Malaysia. *International Journal of Advanced Science and Technology*, *29*(6), 391-397.

Kaspersky. (u.d.). Tips on how to protect yourself against cybercrime. Retrieved from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.

Kemp, S. (2020). DIGITAL 2020: JULY GLOBAL STATSHOT. Datereportal. Retrieved from https://datareportal.com/reports/digital-2020-july-global-statshot.

Lenhart, A. (2015). Social Media and Teen Friendships. Retrieved from https://www.pewresearch.org/internet/2015/08/06/chapter-4-social-media-and-friendships/.

Malay Mail. (2020). Cops: Single mother in Kelantan loses RM480,000 in love scam. Retrieved from https://www.malaymail.com/news/malaysia/2020/10/10/cops-single-mother-inkelantan-loses-rm480000-in-love-scam/1911511.

Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the Internet on economic growth and prosperity. *McKinsey Global Institute*, *1*(0360-8581).

Morgan, S. (2016). Hackerpocalypse: A Cybercrime Revelation. Retrieved from https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/.

New Straits Times. (2018). People still falling victim to love scam despite awareness campaign. Retrieved from https://www.nst.com.my/news/crime-courts/2018/09/411233/people-stillfalling-victim-love-scam-despite-awareness-campaign.

Orchard, T. (2019). Dating Apps. In Lykins, A. (Ed.), Encyclopedia of Sexuality and Gender, 1-2. doi: 10.1007/978-3-319-59531-3_19-1.

Rose, L. (2012). Online dating clicking with singles, but digital love can have drawbacks: study: Online dating clicks with more singles: study. The Canadian Press.

Saad, M. E., Abdullah, S. N. H. S., & Murah, M. Z. (2018). Cyber romance scam victimization analysis using Routine Activity Theory versus apriori algorithm. *International Journal of Advanced Computer Science and Applications*, *9*(12).

Sanders, J. (2011). Online dating and social media collide. Gadsen Times.

Seal, k. (2020). Global Dating App Usage Increases 82% During Pandemic - Dating Sites Reviews. Datingsitesreviews.com. Retrieved from https://www.datingsitesreviews.com/article.php?story=global-dating-app-usage-increases-82--during-pandemic.

Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1).

Singh, S. (2020). Widow cheated of more than RM1mil in love scam. The Star. Retrieved from https://www.thestar.com.my/news/nation/2020/06/28/widow-cheated-of-more-than-rm1milin-love-scam.

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*, 342-361.

Span, P. (2020). When Romance Is a Scam. The New York Times. Retrieved from https://www.nytimes.com/2020/03/27/well/elderly-romance-scam.html.

Statistics and Facts for Online Dating - Dating Sites Reviews. Datingsitesreviews.com. Retrieved from https://www.datingsitesreviews.com/staticpages/index.php?page=Online-Dating-IndustryFacts-Statistics#ref-GODI-2020-5.

Stewart, S. (2020). Romance scams are on the rise during pandemic. Chron. Retrieved from https://www.chron.com/coronavirus/article/Romance-scams-at-an-alltime-high-during-pandemic-15505121.php.

Stoicescu, M. (2019). The globalized online dating culture: Reframing the dating process through online dating. *Journal of Comparative Research in Anthropology and Sociology*, *10*(01), 21-32.

Sumter, S. R., & Vandenbosch, L. (2019). Dating gone mobile: Demographic and personality-based correlates of using smartphone-based dating applications among emerging adults. *New media & society*, *21*(3), 655-673.

Tan, B. (2019). JB housewife loses RM380,000 in love scam. Malaymail. from https://www.malaymail.com/news/malaysia/2019/12/10/jb-housewife-losesrm380000-in-love-scam/1817866.

Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A., & Varpio, L. (2015). Choosing a qualitative research approach. *Journal of graduate medical education*, *7*(4), 669-670.

Utusan Borneo. (2018). Wanita rugi RM913,504 ditipu 'African Love Scam'. Retrieved from https://www.utusanborneo.com.my/2018/12/09/wanita-rugi-rm913504-
ditipu-african-love-scam.

Weisbaum, H. (2020). Looking for love online? Romance scammers steal your heart to steal your money. Better By Today. Retrieved from https://www.nbcnews.com/better/lifestyle/lookinglove-online-romance-scammers-steal-your-heart-steal-your-ncna1135766.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665-684.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*, 443-455.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, *21*(2), 105-109.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.

Yapp, E. (2020). Malaysia's digital transformation efforts progress. Retrieved from https://www.computerweekly.com/feature/Malaysias-digital-transformation-effortsprogress-amid-challenges.

YouGov. (2017). 3 in 10 Malaysians have used internet dating. Retrieved from https://my.yougov.com/en-my/news/2017/11/23/internet-dating/.

Zahid, (2016). Available at Microsoft Word - 342023 (perdana.org.my).