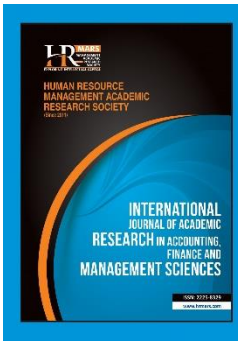


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL

www.hrmars.com
ISSN: 2225-8329

Covid-19 Pandemic and Online Fraud: Malaysian Experience

Ahmad Auzan bin Md Noor, Nor Hafiza Haron, Syed Redzwan Sayed Rohani, Rahayu binti Abd Rahman

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v12-i4/14172 DOI:10.6007/IJARAFMS /v12-i4/14172

Received: *16* October 2022*,* ***Revised:*** *19* November 2022*,* ***Accepted:*** *30* November 2022

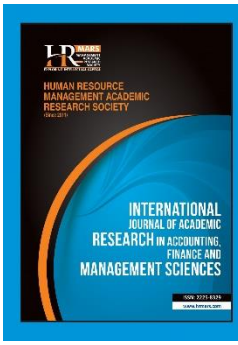
Published Online: *21* December 2022

In-Text Citation: (Noor et al., 2022)

To Cite this Article: Noor, A. A. bin M., Haron, N. H., Rohani, S. R. S., & Rahman, R. binti A. (2022). Covid-19 Pandemic and Online Fraud: Malaysian Experience. *International Journal of Academic Research in Accounting Finance and Management Sciences*, *12*(4), 192–207.

Vol. 12, No. 4, 2022, Pg. 192 - 207

http://hrmars.com/index.php/pages/detail/IJARAFMS | **JOURNAL HOMEPAGE**


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2225-8329

Covid-19 Pandemic and Online Fraud: Malaysian Experience

Ahmad Auzan bin Md Noor[1], Nor Hafiza Haron[2], Syed Redzwan Sayed Rohani[3], Rahayu binti Abd Rahman[4]

[1]Commercial Crime Investigation Division, Royal Malaysia Police, Manjung, Perak, Malaysia, [2]Faculty of Computing and Multimedia, Kolej Universiti Poly-Tech MARA Kuala Lumpur, Malaysia, [3,4]Faculty of Accountancy, Universiti Teknologi MARA, Perak Branch, Tapah Campus, Tapah Road, Tapah, Malaysia

Corresponding Author's Email: rahay916@uitm.edu.com

Abstract

The main objective of this study is to examine how the Covid-19 outbreak has affected online fraud in Malaysia. In particular, this study aims to provide a conceptual discussion as well as a comparison analysis of online fraud patterns prior to and during the Covid-19 outbreak. This study uses police recorded online fraud data to provide comparison between pre and during the Covid-19 pandemic. This study period is 2018-2019 and 2020-2021. Results indicate that most online fraud categories increased dramatically during the Covid-19 outbreak. In particular, the number of online frauds associated with e-commerce and online investment, which are the most common online fraud categories in Malaysia, have seen the largest increasing rates between the two periods. The findings of this study provide preliminary evidences on the increasing of online fraud in the country and can motivate researcher to investigate on the factors that affect such frauds.

Keywords: Malaysia, Online Fraud, Cybercrime, Covid-19 Pandemic

Introduction

Covid-19, which the World Health Organization declared a global pandemic on March 11, 2020, has had a significant impact on society's lives and socioeconomic activities. Most governments throughout the world have enforced national lockdown as an effective measure to stop the spread of the Covid-19 virus, which has affected civilian mobility and normal activities. The first lockdown, also known as a Movement Control Order (MCO), was implemented in Malaysia in March 2020. The order is a form of social repression that restricts citizens' freedom of movement, assembly, and international travel. Non-essential enterprises, industry, government, and educational institutions were also required to close. The shift from an offline to an online paradigm has resulted in severe and unprecedented changes in working patterns, mobility, shopping, and social interaction, resulting in an unavoidable increase in the usage of digital technologies.

According to a statistical analysis by the Malaysian Department of Statistics, the MCO has seen an increase in the number of Malaysians who use the Internet to order goods or

services, seek health information, conduct online banking transactions, take informal or formal online courses, and get information from government agencies. The analysis also reports that the percentage of Malaysians who use the Internet to obtain health-related information or services climbed from 45.2 percent in 2019 to 61.9 percent in 2020. Meanwhile, in 2020, 61.9 percent of Malaysians chose internet banking, a considerable increase from 50.5 percent in 2019. In terms of education, the number of people taking informal online courses climbed to 20.8 percent in 2020, up from 9.5 percent in 2019, while the number of people attending official online courses increased to 18 percent in 2020, up from 8.1 percent in 2019. Purchases of goods or services through e-commerce platforms such as Shoppe, Lazada, and Grab grew to 45 percent in 2020 from 35.2 percent in 2019 (TheStar, 2021).

Prior research has found that Covid-19 has a variety of effects, including on people's health (Boyle et al., 2020; Xiang et al., 2021), e-commerce (Jlkova & Kralova, 2021; Bhatti et al., 2020; Sayyida et al., 2021), education (Daniel, 2020; Kogan et al., 2020), and criminal (Jamil et al., 2021; Buil-Gil et al., 2021; Hawdon, Parti & Dearden, 2020; Tharshini, Hassan, & Mas'ud, 2021; Ashby, 2020). For instance, Jamil et al (2021) point out that Covid-19 and related measures have an impact on both physical and online criminalization. Prior studies (Nivette et al., 2021; Boman & Gallupe, 2020; Ashby, 2020; Campedelli et al., 2021; Gerell et al., 2020; Halford et al., 2020; Hodgkinson & Andresen, 2020; Mohler et al., 2020; Langton et al., 2021) highlight that the nationwide lockdown, which obliged residents to remain at home, had a positive and considerable influence on reducing physical crimes. Nivette et al (2021), for example, investigate the influence of Covid-19 restrictions on six types of physical crimes: assault, burglary, robbery, theft, car theft, and homicide in 27 cities across America, Europe, the Middle East, and Asia. The findings, based on police-recorded crime statistics, reveal that the national lockdown significantly reduces urban physical crimes in all cities. Similar to other countries, in Malaysia, Bukit Aman Criminal Investigation Department reveals that the country's physical crime index decreased by 49.1 percent or 5,098 cases, from March to May 2020, compared to 10,368 cases from January to 10th March 2020 (Bernama, 2020).

Despite its success as a deterrent to physical crime, the restriction movement order failed to prevent cybercrime during the pandemic. The rising usage of digital technology, such as smartphones, laptops, tablets, desktop computers, and smart televisions, has resulted in a surge in online fraud, scams, invasions, and security breaches. Indeed, Jamil et al (2021) argue that the pandemic has created an environment of insecurity, allowing fraudsters to use new technology to commit numerous crimes. As of April 2020, Hamid (2020) reported a 42 percent increase in cybercrime cases in Malaysia, with a total of 4,596 cases.

Several research on the impact of Covid-19 on cybercrime; cyber-dependent and cyber-enabled crimes have recently been published (Buil-Gil et al., 2021; Hawdon et al., 2020; Tharshini et al., 2021; Kemp et al., 2021). Tharshini et al (2021) in Malaysia, for example, give some early evidence on the link between the MCO and cyber-dependent crimes, such as online phishing/malware dissemination, and cyber-enabled crimes; online fraud, and online sexual harassment. In addition, Jamil et al (2021) use a PwC survey on financial crime to show that occurrences of cybercrime in general increased by 37 percent after the national lockdown was implemented. Those findings undoubtedly help to a preliminary knowledge of Malaysia's cybercrime situation, particularly during the Covid-19 outbreak. Nonetheless, Hawdon, Parti, and Dearden (2020) point out that the Covid-19 pandemic has varied effects on different types of cybercrimes. Thus, an equally important issue to examine is the extent and impact of the pandemic on different types of cyber-enabled frauds, also known as online fraud in Malaysia.

E-commerce fraud, Macau fraud, online investment fraud, online loan fraud, and love fraud are the five most prominent types of online fraud in Malaysia, each of which could be affected differently by Covid-19. Hence, this study makes an attempt to improve understanding how Covid-19 and its measures affect each category of online fraud. It also provides a discussion and preliminary comparison analysis of online fraud patterns before and during Covid-19 outbreak in Malaysia.

With the above understanding in mind, this study proceeds with the extant literature on Covid-19 and online fraud relationship in Section 2. In Section 3 we describe the data used in this study as well as the preliminary comparison analysis. Finally, Section 4 concludes with a brief discussion of the findings and some closing remarks.

Literature Review

Prior studies on online fraud during the Covid-19 pandemic

The advent of the internet and related technologies has led cyber-enabled frauds to become a global issue (Button & Cross, 2017; Pandey & Pal, 2020). Cyber-enabled frauds, also known as online fraud, is a type of fraud that involves the use of internet services or software with internet connectivity to defraud or exploit victims (Longe et al., 2009). The revolution in communication and information technologies has opened up new and effective routes as well as chances for fraudsters to carry out various types of frauds on a large scale at low cost both within and outside the fraudster country's boundaries.It has increased the risk of victimization for many persons who would not have been openly targeted with such crimes previously.

Online fraud is a serious threat to people's financial and overall well-being all around the world. Prior research (Whitty, 2018; Whitty & Buchanan, 2012; Alam et al., 2021) has highlighted the financial and non-financial consequences of internet scam victims. Some of them had suffered enormous financial losses, including the loss of all their superannuation, the need to repay loans over time, and the loss of life savings owing to the selling of assets such as cars, houses, and property. Prior research has also indicated that online victims suffer significant emotional and psychological consequences as a result of their victimization. Shame or embarrassment, discomfort, despair, rage, worry, shock, and loneliness were the most common. Furthermore, Button et al (2009) point out that online fraud has a long-term impact on victims, which leads to changes in their behaviour. According to their research, 74.5 percent of online fraud victims change their behaviour and become more careful, apprehensive, and distrustful of others. In addition, victims of online fraud may suffer from a variety of physical illnesses and harmful health implications, such as insomnia, nausea, and weight loss, as a result of their online fraud experience

Covid-19 and its measures exacerbate online fraud patterns (Buil-Gil et al., 2021; Kemp et al., 2021; Buil-Gil & Zeng, 2021). For example, Buil-Gil et al (2021) provide preliminary analysis of the short-term impact of Covid-19 and lockdown measures on online fraud in the United Kingdom. Using police-reported data from May 2019 to May 2020, the findings indicate that cybercrime report cases have risen dramatically during the Covid-19 outbreak. In addition, the results show that online fraud resulting from online shopping and auctions was the most common type of fraud in the UK throughout the outbreak. Furthermore, Kemp et al (2021) aims to provide a better understanding of the relationship between the COVID-19 pandemic and cybercrime in the United Kingdom. The findings indicate that while overall cybercrime and total fraud climbed above predicted levels, the impact of the pandemic on different types of cybercrimes varried. The data show that, whereas cyber-enabled online shopping and love fraud increased, ticket fraud decreased as it depended on events taking

place in physical areas. Meanwhile, concentrating on one type of online fraud, Buil-Gil and Zeng (2021) examine the love fraud trend throughout the pandemic. To achieve the research objectives, the study used police love fraud statistics in the UK, and the Understanding Society longitudinal survey data. Based on auto regressive integrated moving average (ARIMA) modelling, the results show that cyber-enabled love fraud experienced a large increase after April 2020. Furthermore, the findings reveal that the rise in love fraud was more abrupt among young adults than among older people.

Online frauds in Malaysia during the Covid-19 pandemic

Similar to other countries, Covid-19 pandemic also affects the incidents of online fraud in Malaysia. In general, there are five most common types of online fraud occurring in the country namely e-commerce fraud, Macau fraud, online investment fraud, online loan fraud and love fraud.

E-commerce Fraud

The Covid-19 outbreak has accelerated the growth of the e-commerce sector in Malaysia as a result of the shutdown of the majority of retail stores in the country. Furthermore, because citizens are more inclined to take the necessary precautions in preventing the spread of the virus and the ongoing lockdown, the majority of them choose to purchase daily necessities through an e-commerce platform. According to Hasanat et al (2020), the use of online retail applications and e-commerce mobile apps has increased significantly in terms of total number of active users, new users, and payouts since the MCO legislated. In addition, iPrice Group survey data shows that both of Malaysia's main e-commerce platforms, Lazada and Shopee, have seen a significant growth in online visits. Shopee received 81.82 million visitors in the first quarter of 2020, while Lazada received 36.96 million (Zhe, 2020). As a result, Malaysia has been ranked as the 35th largest e-commerce market in the world, with an estimated revenue of $6 billion in 2021 (ecommerceDB, 2022).

However, Gohain (2021) emphasizes that e-commerce is a double-edged sword. Despite the numerous benefits offered, e-commerce platforms and apps with poor and insecure cyber security expose personal information, including banking account information, resulting in a surge in fraudulent activities. According to Cyber Security Malaysia, cybersecurity reported cases increased by 82.5 percent (838 cases) from March 18 to April 7, 2020 (Devanesan, 2020). One of the factors contributing to the upward trend is the country's internet platform's vulnerability. For example, Misirana et al (2021) stress that, despite Shopee's efforts to strengthen the system's security, scammers are actively seeking ways to circumvent the platform's established security mechanisms. Furthermore, they point out that the business model offered by such e-commerce platform is easily exploitable by scammers because the platform does not require vendors to register their businesses with the Malaysian Companies Commission (SSM) and does not conduct background checks. Although this flexibility appears to foster citizen participation in e-commerce, it also encourages more scammers and online fraud.

Consistent with the arguments, Malaysian Domestic Trade and Consumer Affair Ministry statistics indicate that online shopping scams were rampant during the MCO between March and June 2020. According to Bavani (2020), there were 5,415 incidences of e-commerce fraud reported and 2,287 complaints received by June 2020. Profiteering, not showing prices, false representation and deceiving consumers about products, as well as the sale of counterfeit goods and services, were among the incidents (Jusoh & Nizar, 2022). The media such as,

Bernama (2020) highlights that scams involving online sales of face masks during the Covid-19 pandemic caused losses of RM18 million in 2020. Similarly, Hilmy (2020) reports that two people lost RM41,920 in an e-commerce scam via Facebook platform when they tried to buy 700 boxes of face masks online. After seeing multiple Facebook comments claiming that the ordered face masks never arrived, both victims realized they had been duped. The highlighted cases by media suggests that fraudsters have been exploiting an increase in demand for healthcare-related items by duping desperate and vulnerable purchasers through a variety of e-commerce fraud schemes.

Online love fraud

A love scam, also known as a romance scam, is an online fraud that takes advantage of a relationship to obtain financial gain (Whitty & Buchanan, 2012). Scammers pretend to have amorous intentions in order to gain their victims' trust and affection before defrauding them of their money. Love scams, unlike other forms of online fraud, are particularly personal, as victims are drawn in by the romance aspect of the hoax. Whereas victims are usually determined to keep a romantic relationship going, fraudsters' ultimate goal is to get money.While love scams such as newspaper dating classifieds existed before the Internet, newly established mass communication platforms such as social networking sites have been widely used to perpetuate the fraudulent offence in recent years.

According to Hamsi et al (2015), fraudsters frequently use phoney identities to approach lonely and desperate women in search of love and then become their fake partner. Then, once the connection has gained trust, the love scammer would use a variety of tactics to persuade the victim to transfer money to the love scammer's bank account. This transaction may happen to the victim multiple times till they become suspicious or believe it is not a true love relationship.

In line with the popularity of numerous dating applications when the COVID-19 pandemic began, the love fraud incidents also show an increasing trend immediately after the MCO started. According to Perimbanayagam (2021), a forty-four-year-old woman lost nearly her entire life savings of RM2.7 million to an 'American pilot' she met on a social networking site. In a similar vein, Dermawan (2022) notes that a 63-year-old woman lost RM3.9 million after falling prey to a love fraud. Between December 2021 and March 2022, the victim made 184 transactions totaling RM3.9 million into 18 different bank accounts after the man informed her, he had obtained a project at the oil rig and needed money.

Macau Fraud

The Macau fraud has been categorized as a telecommunication fraud. Originating from syndicates in Taiwan and China, the scam has now spilled over across Asia including Malaysia. The most common modus operandi of the scam starts with a phone call from someone pretending to be an officer from a bank, insurance companies, Inland Revenue Board, law enforcement agencies; police, immigration or customs office as well as a debt collection office. The caller then convinces the victim to hand over a huge sum of money by alleging that the victim owes money, has an outstanding fee, or has been accused of committing a crime. For example, the caller may impersonate as a bank officer and claim that the victim has failed to pay their credit card payments. The fraudster then tells the victim that unless he or she transfers money to the scammer within a limited period of time, the victim's bank account would be frozen or blacklisted. Because of the stressful and frightening scenario, as well as

the desire to avoid being blacklisted or having their bank accounts frozen, the victim transfers money to the scammer.

According to Borneo Post (2020), the Royal Malaysia Police (RMP) registered and recorded 5,218 Macau Scam cases in Malaysia from January to October 2020, resulting in projected losses of approximately RM256 million. The victims are predominantly women, with over 3,000 cases involving them, and the majority are over 51 years old. One of the most well-known Macau Scam incidents in Malaysia was the 46-year-old woman who lost more than RM1.2 million. The scam began when she received a phone call from an Etiqa Insurance agent named "Sabrina" in October 2021. Sabrina, the scammer, demanded payment on an RM70,000 insurance policy from the victim.When the victim rejected purchasing the insurance coverage, the scammer diverted the victim's call to the 'Pudu Police Station' to file a police report. The scenario became more problematic when police officers said that the victim was involved in money laundering and murder cases, and that they had issued an arrest warrant for her. The victim is asked to cooperate with the police and report her daily activities, including providing her bank account and credit card information to the officers, in order for the arrest warrant to be lifted. The victim was also told to transfer RM900,000 from her Tabung Haji account (the Malaysian hajj pilgrims fund) to her Bank Islam account and RM200,000 to her Bank Rakyat account by the police officers. When the victim checked the two accounts on April 11 2022, she saw that money had been transferred to the accounts of third parties totaling more than RM1.2 million, she realised she had been duped (MalayMail, 2022).

Online Loan Fraud

Online loan scam was another online fraud that was prevalent during the Covid-19 pandemic. The economic downturn due to the Covid-19 pandemic and its measures, MCO, resulted in many people having lost their jobs, and the business sector has been seriously impacted. The public and business financial difficulties, combined with the strict requirements for licensed financial institutions to approve loans, provide a huge opportunity for non-existent money lending syndicates to promote loans with low interest rates, quick approval, and simple terms in order to attract victims.

In general, the scam has three main characteristics. First, unlike loans issued by legitimate or licensed financial institutions, which do not require the borrower to deposit any money upfront, the victim of an online loan scam will be asked to pay a processing charge. If the bank charges processing costs, the amount charged will be taken from the sanctioned loan amount rather than being required in cash upfront from the borrower. Second, the scammer usually offers a cheaper interest rate or a loan with no interest. The third criteria is that the loan will be approved 100 percent of the time because the borrower's credit history will not be checked.

The most common modus operandi initiated by the scammer is by issuing fake advertisements on social media sites such as Facebook, Twitter, WeChat and WhatsAp, offering their loans at very attractive attributes to lure their victims. In addition, some of the syndicates create fake website links to show up on search engines, when people look for information on loans. To induce credibility, the scammers circulate fake messages with their profile photo and phone number via emails, instant messaging apps, SMS and social media platforms. After the victims express interest in the services, the scammers will call them and request that they pay numerous processing fees before the loan can be approved. The payments include stamping, legal fees, Credit Counseling and Debt Management Agency

payment and Income Tax to secure approval for the loan. After the victims have made the payment, their calls will be blocked.

Recently, there are many online loan scams that have been exposed by the media. According to Bernama (2021), a total of 5,718 cases of non-existent loan fraud were reported in 2020, resulting in losses of approximately RM62 million. This was up from 5,309 cases in 2019, with anticipated damages of RM48.4 million. For example, a 29-year-old businessman suffered a financial loss of RM27,780 for a loan scam through WhatsApp. On April 2, the victim received a WhatsApp message offering money lending services, and he eventually accepted to apply for an RM60,000 loan.The victim was subsequently instructed to deposit the RM27,780 loan processing charge into three separate bank accounts by the scammer.

Online Investment Fraud

Online investment fraud is an illegal deposit taking activity, using internet and information technologies such as emails, websites, Facebook and telegram as a key conduit for engagement, communication, and transaction between scammers and the general public. Scammers are unlicensed or unregistered businesses or individuals who solicit investment funds from the general public by promising fund management advice on investment schemes, securities, or futures.

In Malaysia, online investment scams are not new. In general, the investment fraud scheme has several common features include (i) operators of illicit online investment schemes will claim that their schemes are risk-free or very low-risk, and will provide investment opportunities that are higher than the market rate of return, (ii) In terms of registration, the majority of unlawful operators will either claim to be overseas operators who do not require licenses from Malaysian regulators to operate their businesses, or they will claim to already hold the proper licence from relevant authorities/regulators, (iii) operators will pay unsuspecting victims of these schemes high returns at the initial stage to encourage them to recruit new investors, (iv) the survival of this scheme is dependent upon the recruitment of new depositors, as the scheme use funds obtained from new depositors to pay dividends to the existing depositors, and (v) when the operator believes the plan is about to fail, he will leave with the monies received, putting the depositors on the losing end.

One of the first online investment scams in Malaysia initiated by a scammer named Phazaluddin in 2007. He raised RM65 million from 52,000 investors via the website platform www.danafutures.com. During the Covid-19 outbreak, the country observed a surge in incidents of internet investing. Many investors have had extra time to enter the market as a result of heightened travel restrictions. As a result, the number of novice traders seeking financial advice via the internet has increased, giving scammers more potential victims. Despite the fact that the Malaysian Securities Commission and the Malaysian Exchange, Bursa Malaysia, have encouraged investors to be on high alert and protect themselves from being victims of these fraudulent parties, the media has exposed numerous online investment scams throughout the pandemic. For example, according to Bahaudin (2022), nine people, three men and six women, aged 41 to 62, were imprisoned for operating a non-existent stock investment known as Planetrade Investment (Plan E Investment). The syndicate has been promoting investments based on the purchase of preferential shares since January of 2021. Investors were guaranteed a fixed profit rate of roughly 4% to 5% per month on their capital, as well as the assurance that the money would be invested in various shariah-compliant investing mediums both locally and internationally. However, an investigation revealed no evidence that the parties involved had purchased shares for investment purposes. According to Bukit

Aman Commercial Crime Investigation Department (CCID) director, Datuk Mohd Kamarudin Md Din, aside from providing payouts to investors at an early stage in the form of a pyramid scheme, the money was utilized for personal purposes. The CCID received a total of 21 reports related to this online investment scam, with a total loss of RM3.32 million.

Online fraud in Malaysia: Prior to and during the Covid-19 pandemic-an analysis

Methodology

It is a descriptive study to examine how the Covid-19 outbreak and its countermeasures have affected Malaysia's online fraud patterns. This study uses police reported online fraud data from 2018-2019 to 2020-2021. The main objective of this study is to make a comparison analysis on online fraud patterns before (2018-2019) and during the Covid-19 pandemic (2020-2021). This study divides online fraud incidents in Malaysia into five categories based on Royal Malaysia Police reports: e-commerce fraud, Macau fraud, online investment fraud, online loan fraud and online love fraud.

Results

Table 1 compares online frauds prior to the Covid-19 pandemic (2018-2019) and during the pandemic (2020-2021), and estimates the relative change between the two values for each type of online fraud. The findings demonstrate that the majority of online frauds increased between the two periods, with the increasing rate being particularly substantial in the cases of online investment fraud and e-commerce fraud. Scams in Macau fraud and online loans fraud are also at an all-time high, especially during the pandemic. Love fraud patterns, on the other hand, have decreased during the pandemic era. The modest number of cases reported and recorded by RMP may have contributed to this decline. Overall, the findings show that, with the exception of love scams, all types of online fraud increased significantly during the Covid-19 pandemic compared to before the outbreak.

In addition, Table 1 reveals that the top three types of online fraud in Malaysia for both periods are the same: Macau scam, online loan fraud, and e-commerce fraud, based on the total cases recorded. Nonetheless, the findings in Table 1 and Figure 1 demonstrate that the Covid-19 pandemic has a variety of consequences on various types of online fraud and changes their patterns. Prior to the Covid-19 outbreak, for example, Macau fraud had the greatest recorded cases in Malaysia, with 10,595 cases. However, the pattern changed when the pandemic started, as shown in Table 1, where e-commerce fraud was the most common type of fraud, with 15,424 incidents reported to the Royal Malaysia Police.

Descriptive Results

Table 1

Online fraud incidents in pre-and during the Covid-19 pandemic

Types of online fraud	Pre-Covid-19 pandemic 2018-2019 (Number of cases reported)	During Covid-19 pandemic 2020-2021 (Number of cases reported)	Relative change (%)
E-commerce fraud	6,808	15,424	126.56
Online loan fraud	9,274	10,484	13
Macau fraud	10,595	12,238	15.5
Online investment fraud	2,014	4,850	140.8
Online love fraud	3,229	3,035	-6
Total online fraud	31,920	46,031	44.21

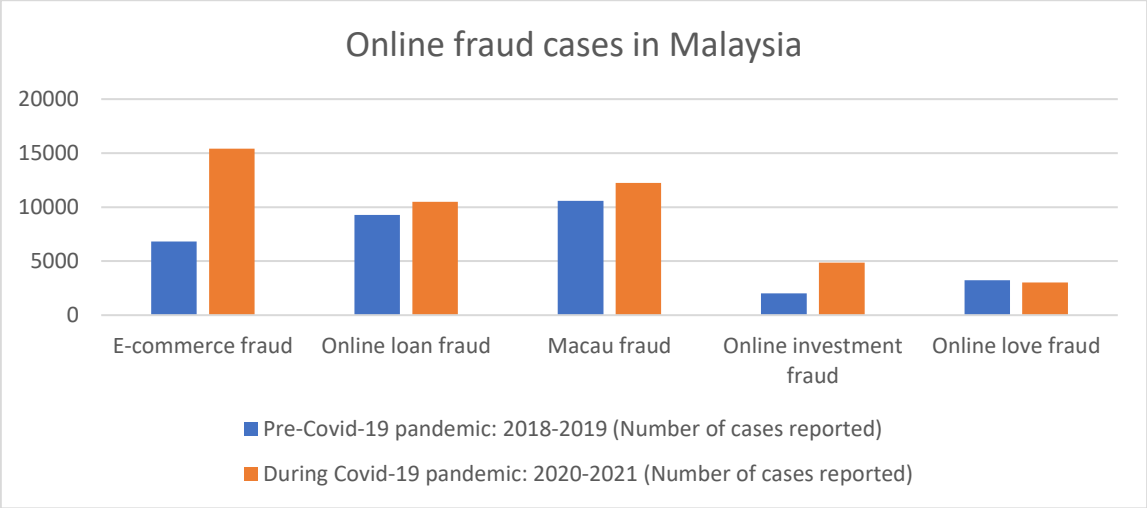


Figure 1 Online fraud patterns prior to and during the Covid-19 pandemic

Furthermore, Figure 2 to Figure 6 report a descriptive year-to-year comparison for each category of online fraud; e-commerce fraud, Macau fraud, online investment fraud, online loan fraud and love fraud from 2018 to 2021, respectively. As illustrated in Figure 2 to Figure 3, e-commerce fraud, and Macau fraud on average keep rising year by year. In fact, the patterns have shown that even before the Covid-19 pandemic both types of fraud cases have been increased. Figure 2 shows the number of e-commerce fraud reports visualised by year between 2018 and 2021. As can be seen, reports of e-commerce fraud show a clear upward trend since 2018, but these suffered a very large increase after 2020, which appears to coincide with the Covid-19 pandemic. In particular, the number of reported cases on e-commerce fraud climbed to 5,839 cases in 2020, increasing by 66.69 percent from 2019. The trend will keep rising in 2021 to 9,585 cases, up from 64.15 percent in 2020.

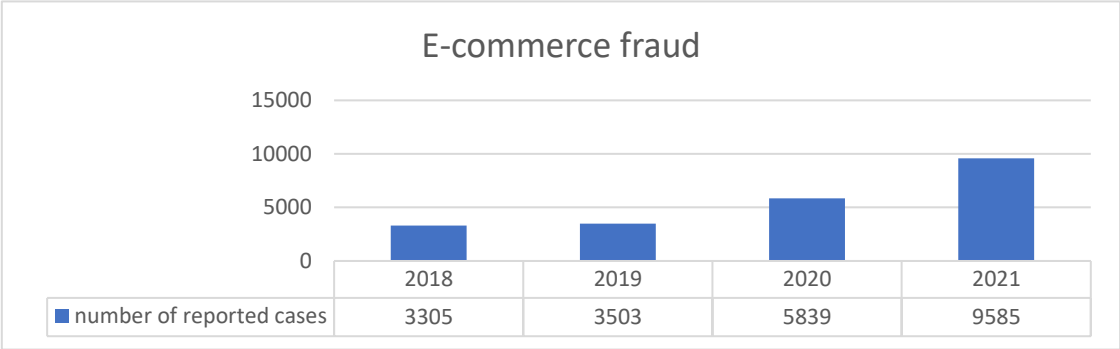


Figure 2 E-commerce fraud patterns prior to and during the Covid-19 pandemic

Similar to e-commerce fraud, Figure 3 also shows the same pattern for Macau fraud. As visualized in Figure 3, the number of reported cases of Macau fraud slightly increased to 6,290 in 2021, up from 10.64 percent in 2019. Meanwhile, Figure 4 show that there was a significant spike in internet investment fraud during the outbreak. For example, in 2019, there were 968 incidents of investment fraud in Malaysia, but by 2021, there will be 3,186 cases, a 229 percent increase.

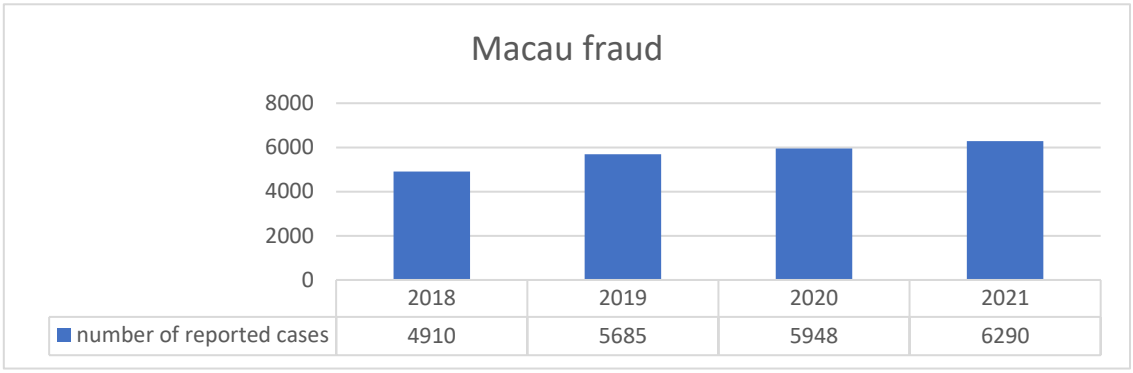


Figure 3 Macau fraud patterns prior to and during the Covid-19 pandemic

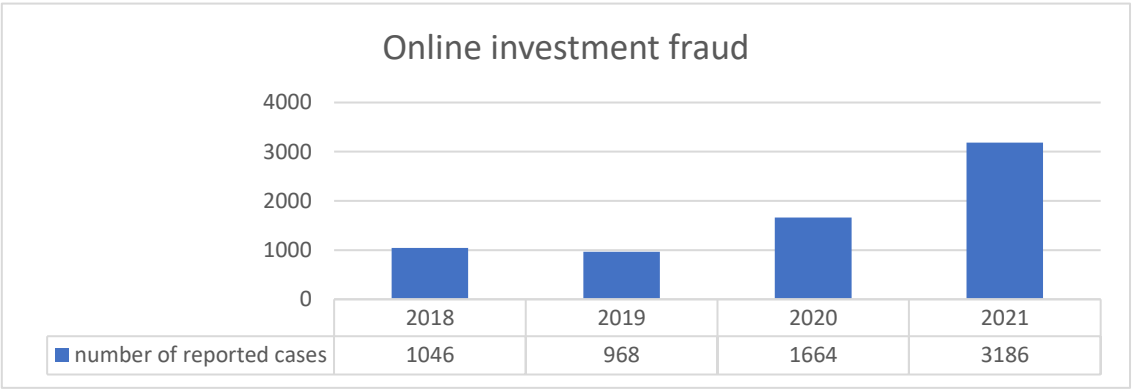


Figure 4 Online investment fraud patterns prior to and during the Covid-19 pandemic

However, as for online loan fraud and love fraud , there were mixed patterns of cases between 2018 to 2021. Figure 5 shows a slight increase by 672 cases from 2019 to 2020. Nevertheless, the cases will decrease to 4,778 in 2021. Similarly, love fraud also shows the same trend, after the national lockdown, the cases slightly rise to 1,577, but decrease to 1,458 in 2021. The mixed patterns open up opportunities for future studies to explore the empirical evidence of these two fraud.

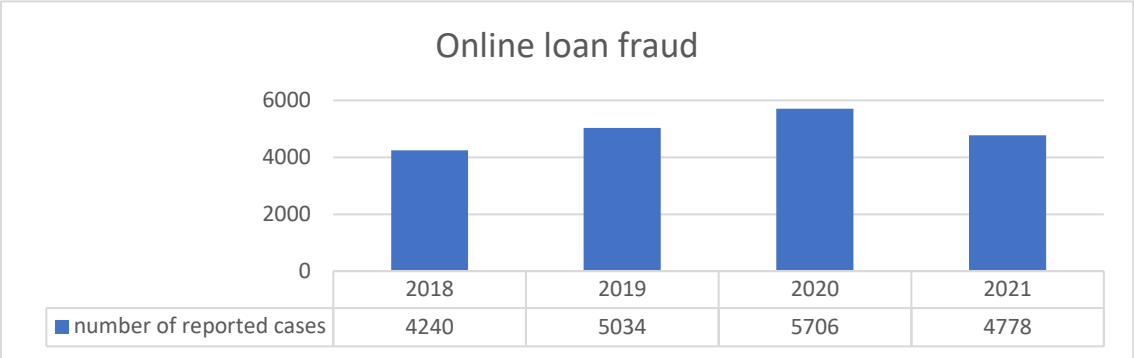


Figure 5 Online loan fraud patterns prior to and during the Covid-19 pandemic

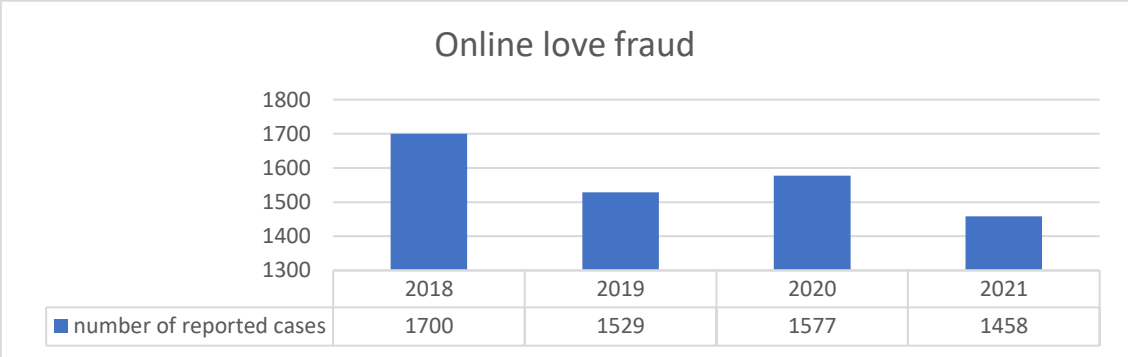


Figure 6 Online love fraud patterns prior to and during the Covid-19 pandemic

In general, the descriptive year-to-year comparison broadly confirms the main findings of this study that the Covid-19 pandemic affects the criminalization pattern. However, further analyses are needed to disentangle whether the observed increase in e-commerce fraud, Macau fraud, online investment can be attributed to the Covid-19 pandemic or is simply a continuation of the upward trend observed in previous years.

Conclusion

This study presented comparative analyses of police-recorded online fraud patterns in Malaysia before and during the Covid-19 pandemic. The findings show that as a result of the Covid-19 pandemic, the reported incidents and rates of online fraud have changed dramatically. The aggregate increase in online fraud before (2018-2019) and during the outbreak (2020-2021) was 44.21 percent across all categories. This suggests that the rising rates of online fraud incidents are a result of substantial changes in people's lifestyles and mobility as they transition from a physical to an online environment, creating enormous opportunities for cybercriminals (Lallie et al., 2021).

Across all online fraud categories, there has been a significant increase in police-recorded e-commerce frauds. The number of recorded cases of e-commerce fraud increased by 173.62 percent from 3503 in 2019 (the year before the pandemic) to 9585 in 2021 (during the epidemic). The findings support the Crime Opportunity Theory, which states that crime levels and types shift rapidly in response to changing opportunity structures and constraints (Nivette et al., 2021). As Covid-19 pandemic and its movement restrictions resulted in the shutdown of the majority of retail stores in the country, the e-commerce sector in Malaysia grew rapidly, encouraging Malaysians to purchase daily necessities, including healthcare-related items, through an e-commerce platform. This gives advantages to the fraudsters to

create a variety of e-commerce fraud schemes. The findings are consistent with prior studies (Buil-Gil et al., 2021; Kemp et al., 2021) in other research settings that have documented an increase in cases of online shopping fraud throughout the outbreak.

While the findings of this study add to better understanding of the impact of the Covid-19 pandemic on cybercrime, it is not without limitation. Because of the reliance on police-recorded data, the results may be biased for generalization purposes.

Prior studies highlight police-recorded data is associated with issues of underreporting since the data is dependent on the victim's willingness to disclose crimes to police (Caneppele & Aebi, 2019; Kemp et al., 2020). Given that, future research should consider other alternative sources to complement and validate the results of this study.

Acknowledgements

The authors would like to thank the Royal Malaysia Police for sharing the data used in this study.

References

Alam, N., Dhillon, G., & Oliveira, T. (2021). Psychological Antecedents and Consequences of Online Romance Scam Victimization Fear.

Ashby, M. P. (2020). Initial evidence on the relationship between the coronavirus pandemic and crime in the United States. *Crime Science*, *9*(1), 1-16.

Bahaudin, N.H. (2022), "'Datuk Seri' nabbed over fake investment scam [NSTTV]", News Straits Times, 4 March 2022, available at: https://www.nst.com.my/news/crime-courts/2022/03/776855/datuk-seri-nabbed-over-fake-investment-scam-nsttv (accessed 5 April, 2022).

Bavani (2020), "6,187 scammed by online sellers", The Star, 20 July 2020, available at:www.thestar.com.my/metro/metro-news/2020/07/20/6187-scammed-by-online-sellers (accessed 20 May, 2022).

Bernama (2020), "5,218 Macau scam cases reported this year, losses estimated at RM256 million", The Borneo Post, 17 November 2020, available at: https://www.theborneopost.com/2020/11/17/5218-macau-scam-cases-reported-this-year-losses-estimated-at-rm256-million/ (accessed 5 April, 2022).

Bernama (2020), "Home Ministry: RM18m lost to online face mask scams amid Covid-19 pandemic", The MalayMail, 17 August 2020, available at: https://www.malaymail.com/news/malaysia/2020/08/17/home-ministry-rm18m-lost-to-online-face-mask-scams-amid-covid-19-pandemic/1894600 (accessed 5 April, 2022).

Bernama (2020), "The crime index down almost 50 per cent during MCO", Bernama, 7 May, 2020, available at: www://bernama.com/en/general/news_covid-19.php?id=1839260 (accessed 20 May, 2022).

Bernama (2021), "Bukit Aman: Non-existent loan fraud on the rise in Malaysia", The Malay Mail, 19 May 2021, available at: https://www.malaymail.com/news/malaysia/2021/05/19/bukit-aman-non-existent-loan-fraud-on-the-rise-in-malaysia/1975406 (accessed 5 April, 2022).

Bernama (2022), "Kedah company manager loses over RM1.2m to Macau scammers", The Malay Mail, 19 April 2022, available at: https://www.malaymail.com/news/malaysia/2022/04/19/kedah-company-manager-loses-over-rm1.2m-to-macau-scammers/2054478 (accessed 5 April, 2022).

Bhatti, A., Akram, H., Basit, H. M., Khan, A. U., Raza, S. M., & Naqvi, M. B. (2020). E-commerce trends during COVID-19 Pandemic. International Journal of Future Generation Communication and Networking, 13(2), 1449-1452.

Boman, J. H., & Gallupe, O. (2020). Has COVID-19 changed crime? Crime rates in the United States during the pandemic. American journal of criminal justice, 45(4), 537-545.

Boyle, C. A., Fox, M. H., Havercamp, S. M., & Zubler, J. (2020). The public health response to the COVID-19 pandemic for people with disabilities. Disability and Health Journal, 13(3), 100943.

Buil-Gil, D., & Zeng, Y. (2021). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23(sup1), S47-S59.

Button, M., & Cross, C. (2017). Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. In The Routledge handbook of technology, crime and justice (pp. 78-95). Routledge.

Campedelli, G. M., Aziani, A., & Favarin, S. (2021). Exploring the immediate effects of COVID-19 containment policies on crime: an empirical analysis of the short-term aftermath in Los Angeles. *American Journal of Criminal Justice*, *46*(5), 704-727.

Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice, 13(1), 66-79.

Daniel, S. J. (2020). Education and the COVID-19 pandemic. Prospects, 49(1), 91-96.

Dermawan, A. (2021), "Widow losses RM3.9 million to 'Korean man' in love scam [NSTTV]", News Straits Times, 21 March 2022, available at: https://www.nst.com.my/news/crime-courts/2022/03/781795/widow-losses-rm39-million-korean-man-love-scam-nsttv (accessed 5 April, 2022).

Devanesan, J. (2020), "Cybersecurity is top concern, as online threats mount in Malaysia by 82.5%", News Straits Times, 14 April 2020, available at: https://techwireasia.com/2020/04/cybersecurity-is-top-concern-as-online-threats-mount-in-malaysia-by-82-5/ (accessed 5 April, 2022).

ecommercedb. (2022), "The eCommerce market in Malaysia", available at: https://ecommercedb.com/en/markets/my/all#:~:text=Malaysia%20is%20the%2035th%20largest,for%20eCommerce%20continue%20to%20increase (accessed 5 April, 2022).

Gerell, M., Kardell, J., & Kindgren, J. (2020). Minor covid-19 association with crime in Sweden. Crime Science, 9(1), 1–9.

Gohain, M. (2021). Impact of covid-19 on malaysian e-commerce. International Journal on Recent Trends in Business and Tourism (IJRTBT), 5(4), 8-10.

Halford, E., Dixon, A., Farrell, G., Malleson, N., & Tilley, N. (2020). Crime and coronavirus: Social distancing, lockdown, and the mobility elasticity of crime. Crime Science, 9(1), 1–12.

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.

Hasanat, M. W., Hoque, A., Shikha, F. A., Anwar, M., Hamid, A. B. A., & Tat, H. H. (2020). The impact of coronavirus (COVID-19) on e-business in Malaysia. Asian Journal of Multidisciplinary Studies, 3(1), 85-90.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. American Journal of Criminal Justice, 45(4), 546-562.

Hilmy, I. (2020), "Two victims cheated of RM41,920 in online face mask scam", The Star, 12 April 2020, available at: https://www.thestar.com.my/news/nation/2020/04/12/two-victims-cheated-of-rm41920-in-online-face-mask-scam (accessed 5 April, 2022).

Hodgkinson, T., & Andresen, M. A. (2020). Show me a man or a woman alone and I'll show you a saint: Changes in the frequency of criminal incidents during the covid-19 pandemic. Journal of Criminal Justice, 69, 101706.

Jamil, A. H., Sanusi, Z. M., Yaacob, N. M., Isa, Y. M., & Tarjo, T. (2021). The Covid-19 impact on financial crime and regulatory compliance in Malaysia. Journal of Financial Crime.

Jilkova, P., & Kralova, P. (2021). Digital consumer behaviour and ecommerce trends during the COVID-19 crisis. International Advances in Economic Research, 27(1), 83-85.

Jusoh, W. N. H. W., & Nizar, N. M. S. (2022). Online scams awareness among muslim university students in malaysia. Journal of Islamic, 7(43).

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. Journal of Contemporary Criminal Justice, 37(4), 480-501.

Kogan, M., Klein, S. E., Hannon, C. P., & Nolte, M. T. (2020). Orthopaedic education during the COVID-19 pandemic. The Journal of the American Academy of Orthopaedic Surgeons.

Kwang Zhe (2020), "Shopee beats Lazada in 1Q20 in Malaysia in website visits", The Edge Market, 29 April 2020, available at: www.theedgemarkets.com/article/shopee-beats-lazada-1q20-malaysia-website visits (accessed 20 May, 2022).

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248

Langton, S., Dixon, A., & Farrell, G. (2021). Six months in: pandemic crime trends in England and Wales. *Crime science*, *10*(1), 1-16.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. Journal of Information Technology Impact, 9(3), 155-172.

Misirana, M., Tan, S. E., Saw, P. H. A., Subri, N. A. M., Darus, N. S. A., Yusof, Z. M., & Ahmad, N. (2021). Early Detection Method for Money Fraudulent Activities on E-commerce Platform via Sentiment Analysis. Journal of Entrepreneurship and Business, 9(2), 121-142.

Mohler, G., Bertozzi, A. L., Carter, J., Short, M. B., Sledge, D., Tita, G. E., Uchida, C. D., & Brantingham, P. J. (2020). Impact of social distancing during covid-19 pandemic on crime in Los Angeles and Indianapolis. Journal of Criminal Justice, 68, 101692.

Nivette, A. E., Zahnow, R., Aguilar, R., Ahven, A., Amram, S., Ariel, B., ... & Eisner, M. P. (2021). A global analysis of the impact of COVID-19 stay-at-home restrictions on crime. Nature Human Behaviour, 5(7), 868-877.

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management, 55, 102171.

Perimbanayagam, K. (2021), "Woman loses RM2.7 million in love scam to 'American pilot'", News Straits Times, 16 April 2021, available at: https://www.nst.com.my/news/crime-courts/2021/04/682894/woman-loses-rm27-million-love-scam-american-pilot (accessed 5 April, 2022).

Sayyida, S., Hartini, S., Gunawan, S., & Husin, S. N. (2021). The impact of the COVID-19 pandemic on retail consumer behavior. Aptisi Transactions on Management (ATM), 5(1), 79-88.

Tharshini, N. K., Hassan, Z., & Mas'ud, F. H. (2021). Cybercrime Threat Landscape amid the Movement Control Order in Malaysia. International Journal of Business and Society, 22(3), 1589-1601.

TheStar. (2021), "Internet access usage increase to 91.7% in 2020", The Star, 13 April, 2021, available at: www.thestar.com.my/business/business-news/2021/04/13/internet-access-usage-increase-to-917-in-2020 (accessed 20 May, 2022).

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.

Xiang, Y., Jia, Y., Chen, L., Guo, L., Shu, B., & Long, E. (2021). COVID-19 epidemic prediction and the impact of public health interventions: A review of COVID-19 epidemic models. Infectious Disease Modelling, 6, 324-342.