



UTM
UNIVERSITI TEKNOLOGI MALAYSIA

FAKULTI SAINS SOSIAL DAN
KEMANUSIAAN

UHMS 1182 (PENGHAYATAN ETIKA & PERADABAN)

SEMESTER 1, 2020/2021

TUGASAN KUMPULAN

NAMA AHLI KUMPULAN :

MUHAMMAD DANIEL HAZEEM BIN MOHAMAD FARDROS

MEK ZHI QING

NG YEN THONG

SAYANG ELYIANA AMIERA BINTI HELMEY

ZEREEN TEO HUEY HUEY

NO MATRIK:

B20EC0026

A20EC0077

A20EC0107

A20EC0143

A20EC0173

DISERAHKAN KEPADA:

DR. ANA HAZIQAH A RASHID

SKEMA PERMARKAHAN (DIISI OLEH PENSYARAH)

KRITERIA	MARKAH
PENDAHULUAN	/2
FAKTOR-FAKTOR	/5
KESAN-KESAN	/5
KESIMPULAN	/2
RUJUKAN	/2
REFLEKSI KENDIRI	/1
LAMPIRAN	/1
MEKANISME PENULISAN	/2
JUMLAH	/20

CONTENT

A. Introduction	2
B. Factor	3
C. Impact	6
D. Conclusion	8
E. Reference	12
F. Self-Reflection	15
G. Attachment	17

GROUP ASSIGNMENT

A. Introduction

In this era of globalization, it is easily for people to excess the internet. All types of information can be found online by different platform such as the most popular search engine, Google and the social media platform used by people. The internet boosts the use of social media platform since 2004, the time of first social media site, MySpace start to rise. The revolution is keep going as the different social media platform is create such as Facebook, Whatsapp, Instagram, Twitter and TikTok. In 2010, Facebook become the largest social media platform in the world as in that time, it has around 517.75 million. Until 2019, this achievement is never snatched by others with the total users of Facebook in 2019 is around 2.26 billion. (Ospina, 2019). To be a Facebook account holder, you are required to fill in your detail like your name and birthday to determine your age. All information relayed to you can be found by others user in Facebook when you are open access to everyone or tag by your friend. Throughout the social media platform, everyone can share their happiness to their friend by using handphone, computer, laptop and so on.

However, the privacy of users is being challenge when they put afford to share the personal information to others in the social media platform. When we want to upload something in our timeline, others can be seen what happen surrounding us. For example, I upload the travel photo in Facebook, then everyone who come to visit my homepage or subscribe my account will know I am currently in travelling. This may be good for those who want to share their happiness to their Facebook friends, but this is a question for us, is social media platform can totally protect us from hackers? Although the social media platform has their own agreement on the protection of user's privacy, the stealing personal information is still happening. (Trepte, 2015). We cannot know who already saw our post and who will be the one stealing our information.

Actually, there are some selection for the social media platform user to protect their privacy. When user access the site, they have been requested to enable the third parties access. (Felt, 2008). If the user is not allowing the site to use their personal information, the site will be unable to get the information. From that, we can protect ourselves from being the prey of scammer. Be careful when give the access of our personal information to the unknown site. Many people just give the access unconsciously because they are interested to the message in the website. The

scammer uses this trait to get their prey. That is why the internet fraud is active in these current years.

We can often see the post in experience on the internet fraud but there are still many social media users confuse about the internet fraud. According to University of Southern Indiana (n.d.), fraud is an unmoral activity by using illegal method to get their own benefit or for their institution's profit. Generally, the fraud can be due to three major element which are opportunity, pressure, and rationalization. One of the examples is cause by personal financial problems as they think they are unable to get the solution for their problem and hence, the idea of illegal activity is carried out. Majority of their target victim is exacted for money or some valuable things such as gold chain. As one of the fraud categories, internet fraud also gives a huge impact in our society.

Internet fraud become the common scams and crimes in world. Refer to the recorded case, up of millions of dollars had been steal by the scammer in the online platform. ("Internet Fraud", 2016). The modus operandi of the scammer is just using the social media to find out all the information they need and use it to steal away all the things they want from your hand. That is why the social media can be one of the ways to facilitate the fraud. By using the social media platform, the scammer can easily find your personal detail such that your email, handphone number and password. Once they get your bank account password, your money save in bank will be steal anytime and anywhere. You cannot do nothing to your money and the only thing you can do is make a police report. Therefore, we need to be more understanding about the misuse of social media platform in the way to facilitate fraud.

B. Factor

One of the factors that cause the misuse of social media platform to facilitate fraud is the high usage of social media among people nowadays. Many people prefer to use social media in most of the aspects of their daily lives such as buying essential things. They feel online shopping is more convenient compared to buy at the physical shop. In the aspect of getting information, they also use social media as the main medium to get information. (Sara, 2020). The high usage of social media in these aspects let the fraud thinks that social media is a suitable platform for them to carry out a scheme to cheat the users. Since most of the people prefer online shopping through social media. The fraud case that most often occur is the users pay to the fraud, but they do not get

the things they want to buy. The fraud chooses social media to carry out this scheme as many teenagers easily believe to the seller which is the fraud and bank in the money without asking opinion of their parents. There is a teenager cheat by the fraud through Whatsapp that he can buy Play Station 5 at a cheaper price by bank in around RM3400, but the teenagers do not get the parcel later and he is “blocked” by the fraud after bank in the money. (Imran, 2020).

Next, the misuse of social media platform to facilitate fraud is also caused by the easiness to spread inaccurate information on the social media platform. Most of the people will share the information on the social media without confirming the truth of the information. This will help the fraud to carry out their scheme more easily. For example, the fraud may use a fake picture and account to appeal everyone to donate for saving a girl with cancer and need a huge amount of money in order to carry out a surgery. Many people will feel pathetic to the girl and start to share the information hoping that more people can help the girl. Most of them do not confirm whether it is a truth or a scheme by the fraud. The fraud can use a blank template of a fund-raising permit to carry out a fraudulent charity donation. (Jean, 2020). The frauds can also create an account on the social media by using a fake identity to let people believe them. The fraud can create a good image in front of the users of the social media and let people fall into his scheme. When the fraud uses his fake identity as a rich CEO, users on social media will assume that the fraud is very rich, and they do not have to afraid that the fraud may cheat them and take away all their money. In fact, everyone should be aware of the information that spread on the social media and do not share the information if you cannot determine it is a truth of fake news to prevent the scheme of fraud.

Furthermore, the easiness of getting personal information from the social media also causes the misuse of social media platform to facilitate fraud. Most users of social media will voluntarily expose their personal information to the public. This will become the easiest way for the fraud to get information about the users. The fraud can get information such as the users’ address, birthday, and their friends. Through the information, the fraud can carry out scheme to the users’ relatives and friends. The most common case is the fraud will create a new account on social media by using the users’ information. (Bernama, 2020). Then, the fraud will add all the users’ friends and family according to the friend list of users on the social media. With the use of this fake identity, the frauds may get more information they want and easily gain the trust from the users’ family and friends. Hence, the social media users should always alert with the person who requires telephone

numbers and money from you through social media even the person is your family members. The fraud can be prevented by just a simple phone call to your family and friends before sending any information and money through social media.

Besides, the misuse of social media platform to facilitate fraud is caused by the attraction of earn money in a shorter time. This occurs among most of the teenagers nowadays that want to buy luxury brand and follow the trend. When their parents cannot afford the huge amount of money required by the teenagers, they might think to earn the money in a wrong way such as through fraud. The teenagers will think the social media is a safe platform for them to fraud as they can use a fake identity. The spread of inaccurate information may also lead the teenagers to a wrong concept that carry out fraud through social media is not a serious case. If nobody stops them on time, they may need to take the legal responsibilities. One of the frauds through social media that usually done by the teenagers is the phishing scam. Phishing scam is the creation of a link to the website that is similar to the official website, but it is actually fake. When the social media users key in their passwords, the fraud can steal the information and change their passwords to transfer the money. (Nur Hanani, 2020). The social media users should always remember not to tell others their OTP from bank and only log in to the bank after making sure it is an official website. If there is any suspicious transfer through bank account, contact the bank quickly by calling the hotline before all your money is lost.

The negative influence by friends also lead to the misuse of social media platform to facilitate fraud. When our friends carry out fraud through social media and gain some benefits, they may try to pursue us to join them so that we can gain the benefits together. If we are being attracted by the benefits, we will also carry out fraud on the social media. Even we are not attracted by the benefits, we may join them because of peer pressure. We afraid of being left behind and alone, so we join them although we know fraud is not true. They will invite us to join them so that they can expand their fraud to more people. (Gail, 2020). Most of the fraud on social media is not carry out by a single person, it is carried out by a team of people. The team will have a strategy on how to carry out scheme to fraud more people.

C. Impact

The only positive side effect of social media fraud is that it spreads awareness amongst social media users. There are billions of social media users globally and not everyone has the same experience as others who got scammed on social media hence the awareness. The person involved would create awareness to others about a social media fraud that they have experienced. (International, 2019). Young people are most likely not fall into the traps that the fraudsters has laid but there is also elderly that use social media and they might not be aware of the frauds that they could get involved with. (ACFE,2020). Social media scammers are most likely to target elderly individuals (age 50 and above) because they are more trusting to a stranger than youngsters. (Calyptix,2015). (Silver,2020). In order to make the minority of social media users or the naïve segment of social media user not getting involved into a fraud, awareness about the issue must be made. Awareness of this issue can be issued through the social media posts or blogs. (International, 2019). Social media users can read and extract information from the posts and educate themselves about the issue. This will most likely help them to identify a way to detect a fraud and how to avoid them. While we are saying that elderly is easier to get scammed, but it does not mean that youngsters would not get scammed either. There is a study about a financial scam that has the millennials at the top of the chart as a victim, hence not only elderly can get scammed but younger people as well. (Guzman, 2018). As a result, awareness is really important to make sure that people know how to browse the social media safely and they will get the gist of what actually is a social media fraud so they would not fall into it without they notice. Without awareness, social media users would never know about how dangerous social media fraud actually is and might getting scammed themselves. As the Portuguese proverb, *“The person who is well prepared has already won half of the battle”*. So, make sure to educate yourself about the issue in order to avoid it.

One of the biggest negative impact of misuse of social media is identity theft. We often hear a lot of this kind of case especially in this technological era. Investopedia define identity theft as the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. (Kagan, 2020). Identity theft often happens when the identity thieves steals users’ personal information such as bank account number and credit card information through any high-tech tactics which entail hacking company databases in order to steal consumers information lists. Identity theft victims

often do not know that their identity was stolen until they start getting calls from creditors or turned down because of a poor credit score for a loan.

Other negative impacts of misuse of social media to facilitate fraud is internet scams which led to identity theft on social media users, this action is also known as phishing. The aim of a scam is to trick people into splitting money or disclosing confidential personal data that can then be used for financial gain, such as email addresses, passwords, and birth dates. However, the approaches may be differed. Most of the scams fall into three main groups. Which are e-commerce scams – fraudsters may claim to be a genuine and trusted online seller on sites such as Instagram and Facebook and consumers pay for the items that turn out to be counterfeit or the items will never arrive, investment scam - fraudsters are always put an interesting advertisement on investment opportunity which are too good to be true which lead consumers who are willing to invest lose some of their money or all of it, and imposter scams - fraudsters act as real brands, real friends or relatives, in order to gain the trust of a customer asking them to buy items, send money or click on links that download malware to their device.

From those group of categories mentioned above, anyone among the social media users in terms of age or gender can be the victims. However, most if the fraudsters are intelligence enough to target at any specific demographic groups as they think these groups are eager to increase their assets and to look more powerful with the wealth they have. For example, Trading Standards in the UK reports that young men are the most likely to be targeted by online scams involving steroids, while middle-aged women are most likely to be targeted by scams involving diet pills, and younger people seem the most likely to be targeted by cryptocurrency scams. In all our society level, these three groups are the main target for the scammer. (International, 2019). Without realized anything, this kind of financial losses may change 360 degrees of their lives.

Nowadays, there are many online dating platforms available such as Bumble, Tinder, OKCupid and many more which online friendship and relationship can develop in a split second. Little did they know that this kind of relationship is highly risk as they do not know each other's backgrounds and have never meet before. Most of the sites are legitimate, but some fraudsters take advantage of this and slowly start asking for cash allegedly to get them out of a desperate situation, with the amounts increasing steadily. And the partners on the other side tend to trust them and

simply bank in the money without knowing any specified reason. They do not realize that they have been deceived by the fraudsters and faced a huge number of losses.

Besides, misuse of social media to facilitate fraud could lead to a distance and create a community division as the fraudsters act as a keyboard warrior which add fuel to the fire. It may seem something enjoyable for them but for the other social media users, it is a huge of never ending misunderstand. Without much of a stretch, fraudsters can ruin the reputation of any users just by making a false story and spreading online through social media. This prompts obsession. The emphasis and consideration of a particular false story may be occupied by spending endless hours on the fraudsters themselves. In comparison to taking it in the down to earth knowledge and skills of everyday life, it depends on primarily creativity and wise use of society while using social media.

Moreover, misuse of social media to facilitate fraud will worsening and toppling economy. In this case, fraudsters may be one of any company rivalries. They act to badmouthing their rivals on social media and leads other people to boycott from using their products and keep a distance from being their business partner. Social media is not entirely risk-free in industry considering that a large number of fans and followers are required to post their feelings to a specific event. The company may be disappointed by this negative remark. With limited government supervision and industry requirements low number of social 'shares' could affect the credibility of a company on others' perspectives as they though that company produce a low-quality product. This will cause a huge loss for them and all the staffs in the company would lose their job as they could not receive any payment.

D. Conclusion

To conclude, we learnt that the misuse of social media platform to facilitate fraud is happening because of the high usage of social media among people, the easiness to spread inaccurate information and getting others' personal information on the social media platform, the attraction of earning money in a shorter time as well as the negative influence by friends. Besides that, this issue brings positive impact that it spreads awareness among social media users. On the other hand, it can cause negative impact like identity theft, phishing problem, and getting fake

friends to the users. It is also leading to a distance and create a community division, worsening and toppling economy as well as affecting the victims' mental health for a long term.

As a prevention from being the victim of online frauds, we can always keep our computers and mobile devices up to date. This method can ensure they are having the latest security system on time and not in arrears. The security systems can help to detect the viruses, malware, and other threats to stop them from invading and stealing our personal data. Without a complete security system, scammers or hackers can easily hack into our computers or devices to get information that benefits them such as our online banking passwords, our social media accounts passwords and so many. We need to update the systems regularly to ensure that its problems and bugs are getting solved on time. If there are no security systems in our devices, we should buy or download the certified systems in order to prevent us from being hacked. This is also important because, there is scammers using very low prices promoting their fake security systems but real hacking systems. Once we got cheated by these people, we are actually paying and welcoming the hackers. So, to prevent all this, we can find for regular and trusted computer shop or technician to help us install a security system.

Besides, we can also use some strong passwords to prevent the outlaws hack into our digital accounts easily. This is stating because there are hackers who hack into our social media accounts then pretend us to borrow money from our families and friends. The more complicated the password, the more difficult they will success to hack and get our information. A strong password should include at least 8 characters, and using not only numbers, but also upper- and lower-case letters, symbols, or special characters. If we use some passwords that are easy to know such as phone number, birthdate, or our names, that will be easy to be guess as this kind of information can always be easily found on our social media. Apart from that, it is also important to not use the same password for all accounts and update the password regularly. This way can effectively help us to increase the safety of our account and personal info.

Other than that, we should also shop on secure websites or only deal with certified merchants. This is because, in this Internet era, online businesses have sprung up like mushrooms after a rain, mixed with those outlaws that try to defraud people's money and then disappear. Without careful screening, we can easily be fooled by these scammers. Thus, we should only trust

those official websites and do research before we deal with them. For example, we can use certified shopping apps like Shopee and Lazada because we are protected under the laws. If there is a website, we can check by looking at its web address begins with https or having a small padlock symbol means it is secured. Besides that, if we want to buy something that is branded, we can deal with their legal or official websites instead of trusting those uncertified ones. In short, shop safely.

Furthermore, we have to be aware of the messages or mails received. This is because, scammers will use this kind of methods, let the users click on the links provided and take the opportunity to invade. Some of them will damage the phone or make it unusable, then steal the data in the device. Worse, there is some of them invade quietly and did not getting notice. They will install certain application that can steal our information and also those passwords we typed in by not discovering by the users. So, when we received this kind of messages, we need to verify its authenticity first. Never click on the links provided or follow the instructions. We must be aware that, typically a formal organization especially bank will not message us personally if there are any bank affairs, let alone using social media platform. Recently there is happening the scammers using WhatsApp to contact the victims and deceive. We need to always remember that, if there is any problem, the formal party will not contact us by phone or social media but formal letters. When we doubt the authenticity of the message or phone call received, we can first call to the bank with its verified phone number and check for the problems.

Moreover, we are recommended to keep our personal information personal. What does it mean? Well, in this era, everyone is using social media. Most of us like to upload our photos, share our lives, and so on, but actually, this action is exposing ourselves to danger. This is because by the social media, the scammers can get our basic information such as birthdate, nickname, school name, place of job, our friends and many more. By these details, they can scam people around us. For example, there is someone get the name, phone number and address of the victim. They keep making harassing calls until the victim shutdown their phone. After that, they pretend as a deliveryman sending a cash-on-delivery package to the victim's house. They will ask their families for money and when their families cannot get to contact with the victim, they just pay for the fraud package. This is only one example, but the tricks of the liar are endless. What we can do is minimizing posting the personal details to social media. Besides, do not expose our social media to public, we can make our accounts private. This is because even if we do not disclose certain

personal information, those who are interested can still find the answers they want from clues. So, beware of everything we posted on social media.

Apart from that, the government can also contribute to reduce this kind of problems. Related ministries or organizations can promote the network real-name system that ensure everyone has only one identity in social media. This is because many of the scammers using fake account to swindle money of others. Some of them pretend as merchant, receiving customers' payment then disappear. Some of them pretend as our families and friends, borrow money from us then vanish. In short, nowadays, ones can have a lot of identity easily through social media. Their ways are ever-changing. Thus, if the government introduce the network real-name system, this can make sure the fake accounts will not be easy to appear. In this way, everyone is using their real name and their accounts must be verified before used. If there is any problem, the related law enforcement officers can also find the party easily as they are using a real account.

In conclusion, online frauds bring serious impact to our society. After understanding how it happens and the effects it may cause, we need to find some ways to overcome them. If we do not take this issue seriously or ignore it, one day our society will be dangerous. So, let's take note of the ways suggested to prevent ourselves from online frauds. Social medias are invented in a good use, thus we must protect it, and at the same time protect ourselves, to ensure that it brings only benefits to us but not harm. In this case, people from all classes should cooperate and work hard together to recover the good and safe environment of the social medias.

E. Reference

- Akram, W. (2018). A Study on Positive and Negative Effects of Social Media. *International Journal of Computer Sciences and Engineering*, 347-354.
- American Bankers Association. (2016). 'Seven tips to avoid online fraud'. *Central Bank*. Retrieved 2020, December 17, from <https://www.centralbank.net/personal/security/security-news/seven-tips-to-avoid-online-fraud/>
- Bernama. (2020, November 20). 'Beware of fake social media accounts created for purpose of fraud, sedition — MCMC'. *The Edge Markets*. Retrieved December 16, 2020, from <https://www.theedgemarkets.com/article/beware-fake-social-media-accounts-created-purpose-fraud-sedition-%E2%80%94-mcmc>
- Calyptix. (2015). 'Internet Crime and Scams from FBI Annual Report'. *CalyptixSecurity*. Retrieved 2020, 19 December, from <https://www.calyptix.com/research-2/internet-crime-and-scams-from-fbi-annual-report/>
- Elderly fraud scams: How They're Being Targeted and How to Prevent It*. (n.d.). ACFE. Retrieved 2020, December 19, from <https://www.acfe.com/fraud-examiner.aspx?id=4294997223>
- Evans, D. and Felt, A. (2008). 'Privacy protection for social networking platforms', *Workshop on Web 2.0 Security and Privacy*, 1-8.
- Gail, C. (2020, December 10). 'How Friends Influence One Another—For Better or Worse—in High School'. *KQED*. Retrieved December 16, 2020, from <https://www.kqed.org/mindshift/57082/how-friends-influence-one-another-for-better-or-worse-in-high-school>
- Guzman, Z. (2018). 'Millennials fall for financial scams more than any other age group'. *make it*. Retrieved 2020, 19 December, from <https://www.cnn.com/2018/03/07/millennials-fall-for-financial-scams-more-than-other-age-groups.html>
- Imran, H. (2020, December 13). 'Doctor, student lose over RM15k to online fraud'. *The Star*. Retrieved December 16, 2020, from <https://www.thestar.com.my/news/nation/2020/12/13/doctor-student-lose-over-rm15k-to-online-fraud>
- International, C. (2019). Understanding The Consumer Experience To Create A Safer Digital World. *Social Media Scams*, 25.

Internet Fraud. (2016). FBI. Retrieved December 19, 2020, from <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud>.

Jean, L. (2020, September 22). 'Teenager pleads guilty to being part of group selling postcards for charity with fake license'. *The Straits Times*. Retrieved December 16, 2020, from <https://www.straitstimes.com/singapore/courts-crime/teenager-pleads-guilty-to-being-part-of-group-selling-postcards-for-charity>

Kagan, J. (2020, November 30). 'Identity Theft'. *Investopedia*. Retrieved 2020, December 18, from <https://www.investopedia.com/terms/i/identitytheft.asp#:~:text=Identity%20theft%20is%20the%20crime,making%20unauthorized%20transactions%20or%20purchases>.

Lewis, K. (n.d.). 'How Social Media Networks Facilitate Identity Theft and Fraud'. *Octane Magazine*. Retrieved 2020, December 17, from <https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud>

Mitchell, T. (2019, July 31). 'How is social media used to commit fraud?'. *Cifas*. Retrieved 2020, December 16 from <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/how-is-social-media-used-to-commit-fraud>

Norton. (n.d.). *Protecting Yourself from Online Shopping Scams*. Retrieved December 17, 2020, from <https://us.norton.com/internetsecurity-online-scams-protecting-yourself-from-online-shopping-scams.html>

Nur Hanani, Z. (2020, December 15). 'Online scams — do not talk to strangers!'. *The Malaysian Reserve*. Retrieved December 16, 2020, from <https://themalaysianreserve.com/2020/12/15/online-scams-do-not-talk-to-strangers/>

Ospina, E. O. (2019, September 18). 'The rise of social media'. *Our World in Data*. Retrieved December 19, 2020, from <https://ourworldindata.org/rise-of-social-media>.

Protect yourself from scams. (2020, April 22). Australian Competition & Consumer Commission. Retrieved 2020, December 16, from <https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams>

Sara, Z. (2020, December 14). 'Social media use increases belief in COVID-19 misinformation'. *WSU News*. Retrieved December 16, 2020, from <https://news.wsu.edu/2020/12/14/social-media-use-increases-belief-covid-19-misinformation/>

Silver, J. (n.d.). 'How to Help Your Parents Prevent Being Scammed as They Get Older'. *ElWell*. Retrieved 2020, 19 December, from <https://www.el-well.com/help-parents-prevent-scammed-older/>

Simplilearn. (2020, November 13). 'Understanding The Impacts of Social Media: Pros and Cons'. *Simplilearn*. Retrieved December 16, 2020 from <https://www.simplilearn.com/real-impact-social-media-article>

Trepte, S. (2015). 'Social Media, Privacy, and Self-Disclosure: The Turbulence Caused by Social Media's Affordances'. *SAGE publishing*, 87-96, doi: <https://doi.org/10.1177/2056305115578681>

What is Fraud?. (n.d.). University of Southern Indiana. Retrieved 2020, December 20, from <https://www.usi.edu/internalaudit/what-is-fraud/>

F. Self-Reflection

Daniel Hazeem:

What I get while writing this is there is actually not many positive effects from the misuse of social media to facilitate fraud. The only positive effect than I can think of actually is awareness about the issue. While there are no positive effects, awareness is actually important and it can help many people from involving themselves with a fraud. Fraud is not a light matter that we can brush it off easily. Therefore, it is better for people to take some useful information from them who experienced in fraud and I believe this will decrease the internet fraud case. While doing some research, I found out that elderly is the most targeted age group for the fraudsters. I am not happy with the fact that they are taking advantage from people who are really vulnerable and hope that this case study can help to avoid themselves from fraud.

Mek Zhi Qing:

Throughout this case study, I realized that there are many causes which lead to the misuse of social media platform to facilitate fraud. Every social media user should be aware of the ways that fraud is carry out so that we will not easily fall into the trap. As a smart user, we should think and identify the truth of a news before sharing it to prevent us become one of the helpers to facilitate fraud on social media. We should also be aware of any suspicious link and do not open it easily due to our curiosity since it may lead to the negative effect to our life.

Ng Yen Thong:

During the process of doing research for this work, I found out there were thousands of people having experienced being deceived. The scammers have made the victims lost their hard-earn money. I feel angry to those who are unwilling to work hard but steal others' result of hard work. This is not the proper way to gain wealth as it is illegal and bring harm to others. Worse, after many years, the fraud cases are not reducing at all but only getting more serious. As a student, I would like to contribute my little strength, in order to help in this issue. We have to totally understand how this problem was happening and what will it brings to our society. People from all classes should cooperate and work hard together so as to recover the good and safe environment of the social medias.

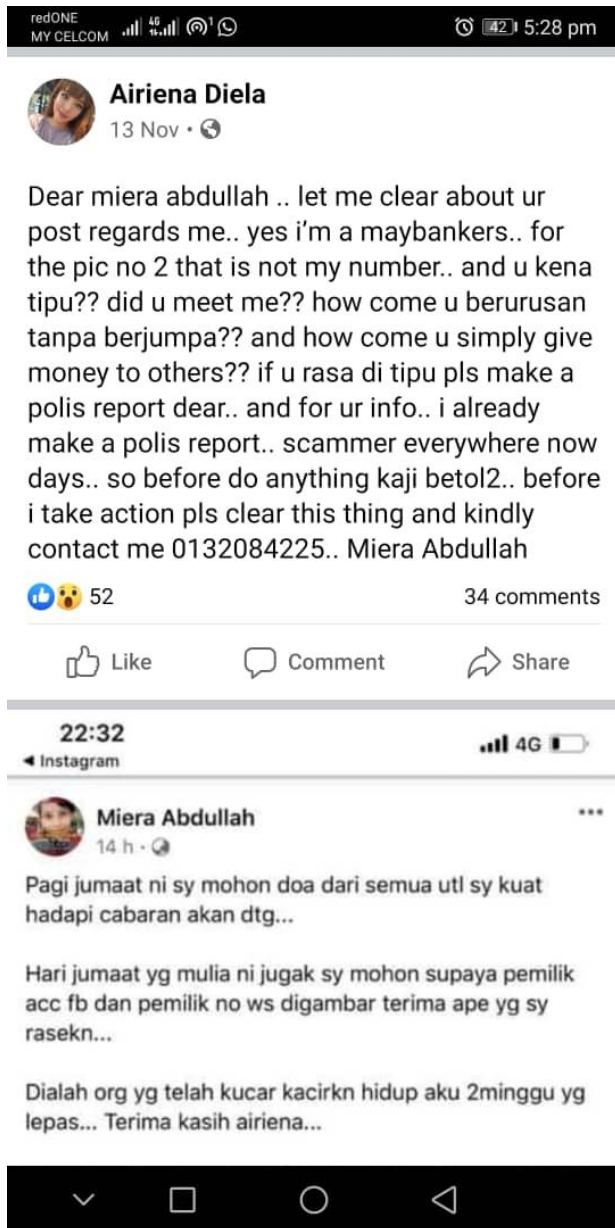
Sayang Elyiana Amiera binti Helmey:

From the throughout research, I realized that people nowadays are one click away from social media. Every single thing happened in their daily lives will be uploaded to social media to express their feelings to others. Unfortunately, there are number of social media users out there use these platforms to facilitate fraud in order to gain something with the suffering of others. It is true that companies that owned these social media platforms has provided many steps of securities to protect each user's information as secured as they can but with high technologies and facilities, fraudsters still can misuse the social media to facilitate frauds. In my point of view, all parties need to work together to raising awareness among users and prevent this problem from keep happening.

Zereen Teo Huey Huey:

From this case study, I become more understanding to the usage of social media. The social media not only give us advantage, but we need to be careful of the following disadvantage. Be aware to what I share and saw in the social media platform. In our group, we also discuss when facing problem throughout this case study. As there are problem facing by our group members, we will discuss in group and vote for the best choice. All of the group member sound out their opinion and give a good cooperation along the group assignment in processing. With the cooperation, we can done this group assignment successfully.

G. Attachment



Source: https://m.facebook.com/story.php?story_fbid=4055590854454401&id=100000105806467

CONGRATULATIONS!
(1) \$1000 Amazon Gift Card
1 is reserved just for you, Facebook User!

Step 1: Click the "CONTINUE" button to claim your prize.
 Step 2: Enter the correct information on the next page to claim your prize.

2 You only have 4 minutes 14 seconds to claim your prize!

amazon **CONTINUE**

1 Unpersonalized phrasing
2 Wording that sounds urgent

Source: <https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/>

Customer Service @Ask_BankCA
 Mr. Smith, sorry to hear you've been having trouble. To better serve you, please visit our site and login. banksite.com/CA/customerservice

John Smith @frustrated-customer
 Help @bank! I can't transfer funds on your website!

Real Bank Account @Ask_Bank **Fake Bank Account @Ask_BankCA**

Source: <https://fortune.com/2016/11/11/social-media-cyber-scam/>

Kena Tipu Scammer Nombor Plat Atas Talian, Mangsa Rugi RM15k

November 19, 2020 By Azizi H — [Leave a Comment](#)

42
PERKONGSIAN

f Facebook

Twitter



SEORANG lelaki berputih mata apabila **kerugian RM15,000** akibat ditipu ketika cuba membeli nombor pendaftaran khas secara atas talian.

Ketua Polis Daerah Seberang Perai Utara, Asisten Komisioner **Noorzainy Mohd Noor** berkata, mangsa berusia 50 tahun itu membeli nombor pendaftaran tersebut menerusi sebuah syarikat di Facebook. Dia juga tidak pernah berjumpa suspek dan segala urusan hanya menggunakan telefon.



Suspek ejen penjual nombor pendaftaran meminta mangsa membuat bayaran secara berperingkat sebanyak tiga kali ke tiga akaun bank berbeza berjumlah RM14,800.

Noorzainy berkata, mangsa mendakwa dia dimaklumkan ketiga-tiga akaun bank tersebut adalah milik 'runner' syarikat yang akan menguruskan pembelian nombor pendaftaran kenderaan tersebut. Dia hanya sedar ditipu selepas gagal menghubungi ejen berkenaan selepas bayaran penuh dibuat.

Berdasarkan semakan dibuat, nombor pendaftaran yang diiklankan itu sudah pun didaftarkan atas nama individu lain. Buat masa ini polis sedang menyiasat maklumat akaun individu terbabit.

SUMBER: **SinarHarian**

Source: <https://pandulaju.com.my/kena-tipu-scammer-nombor-plat-atas-talian-mangsa-rugi-rm15k/>



Gambar hiasan

Warga emas rugi RM61,500 ditipu 'kekasih'

Mohd Rafi Mamat
bhnews@bh.com.my



KUANTAN: Seorang wanita warga emas berputih mata apabila kerugian RM61,500 selepas diperdaya teman lelaknya yang dikenali melalui Facebook, sejak April lalu.

Ketua Jabatan Siasatan Jenayah Komersial negeri, Superintendan Mohd Wazir Mohd Yusof berkata, selepas mangsa berusia 73 tahun yang menetap di Bentong menjalin cinta hampir sembilan bulan.

Katanya, kemudian wanita itu dihubungi teman lelaknya bernama Kelvin untuk meminjam wang RM100,000 yang berjanji akan memulangkan semula.

"Mangsa percaya dengan janji manis itu, memasukkan RM61,500 ke akaun bank atas nama individu lain yang diberikan suspek melalui empat transaksi di kaunter sebuah bank di Bentong.

"Semalam, mangsa datang semula ke bank berkenaan untuk memasukkan baki wang yang dipinjam suspek, namun bernasib baik apabila pihak bank curiga dengan nombor akaun yang digunakan itu sebelum mendapati ia milik scammer," katanya dalam satu kenyataan hari ini.

Katanya, mangsa tampil membuat laporan di Balai Polis Bentong semalam selepas menyedari dia ditipu dan kes disiasat mengikut Seksyen 420 Kanun Keseksaan

Beliau berkata, masyarakat diingatkan supaya tidak mudah terpedaya dengan pelbagai helah seperti itu.

Source: <https://origin.bharian.com.my/berita/kes/2020/12/766753/warga-emas-rugi-rm61500-ditipu-kekasih>