FORM 1

TUNKU ABDUL RAHMAN UNIVERSITY COLLEGE

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

Bachelor of Information System (Honours) in Enterprise Information Systems
Year 2 Semester 2
REI (Group 3)

Cyber crime cases in Malaysia

BACS3033 Social and Professional Issues

2021/2022 (session 202109)

Name (Block Capital)	**Registration No.**	**Signature**	**Marks** (For Lecturer / Tutor use)
1. SOH ZHI YING	21WMR04835		
2. CHIN JOEL FEI	21WMR04802		
3. TAN YIH YEN	21WMR04838	yihyen	
4. LIM TZE YANG	21WMR04819		
5. TAN YIN HUI	21WMR10308		

Lecturer/Tutor's Name: Ms. PREMAWATY A/P MAHINDRA KUMAR

Date of Submission: _____4/12/2021_____

Faculty of Computing and Information Technology

Plagiarism Statement

Read, complete, and sign this statement to be submitted with the written report.

I confirm that the submitted work are all our own work and are in our own words.

	Name (Block Capitals)	Registration No.	Signature
1.	SOH ZHI YING	21WMR04835.	…….
* 2.	CHIN JOEL FEI	21WMR04802.	…….
3.	TAN YIH YEN	21WMR04838.	yihyen …….
4.	LIM TZE YANG	21WMR04819.	…….
5.	TAN YIN HUI	21WMR10308.	…….

Tutorial Group : ……G3……

Date : ……4/12/2021…….

FORM 3

Assignment Final Report Assessment Criteria

The assessment of this final assignment report is based on the following criteria:

Assessment Criteria

Criteria	Excellent	Good	Average	Poor	Score
Part A **Background** **(5%)**	Apparent description about the background of the contemporary topic selected. **(4 - 5%)**	Some part of description about the background of the contemporary topic selected with ambiguity. **(3%)**	Brief description about the background of the contemporary topic selected, which are not directly related to the question. **(2%)**	Very brief description about the background of the contemporary topic selected, which are not related to the question. **(0 - 1%)**	
Part B **Topic analysis and exploration.** **(30%)**	Able to provide apparent and reasonable assessment & justification with very detailed explanations on the chosen topic from social, legal, architecture and market perspectives. Able to look for relevant information from many sources within the duration of time given and well utilize it. **(24 - 30%)**	Good to provide reasonable assessment & justification on the chosen topic from social, legal, architecture and market perspectives. However, some explanations are not clear. Able to look for relevant information from many sources, but some information is not used wisely. **(15 - 23%)**	Average to provide reasonable assessment & justification with a bit of explanation on the chosen topic from social, legal, architecture and market perspectives. Able to look for information from many sources, but some of them are irrelevant. **(8 - 14%)**	Poor to provide reasonable assessment & justification with very little to no explanation on the chosen topic from social, legal, architecture and market perspectives. Able to look for limited information and subject to limited few sources and some information is irrelevant. **(1 - 7%)**	
Part C **Proposed solution(s) for your chosen topic.** **(30%)**	Able to provide an apparent and reasonable evaluation with detailed explanations on the proposed solution(s) for your chosen topic. Able to apply the new ideas and thoughts in solutions and able to use it for autonomous learning. **(24 - 30%)**	Good to provide a reasonable evaluation of the proposed solution(s) for your chosen topic. However, some explanations are not clear. Able to apply new ideas or thoughts in solutions in most situations and able to use them without assistance. **(15 - 23%)**	Average to provide a reasonable evaluation with a bit of explanation of your chosen topic's proposed solution(s). Able to apply new ideas or thoughts in solutions under certain situations and can only use them with some assistance. **(8 - 14%)**	Poor to provide a reasonable evaluation with very little to no explanation on the proposed solution(s) for your chosen topic. Unable to receive & apply new ideas or thoughts on a solution. **(1 - 7%)**	

Summary **(10%)**	Able to provide an apparent summary on the topic chosen. **(8 - 10%)**	Good to provide a summary on the topic chosen. **(6 - 7%)**	Average to provide summary on the topic chosen. **(4 - 5%)**	Poor to provide a summary on the topic chosen. **(1 - 3%)**	
Sub-Total (75%)					

Criteria	Excellent	Good	Average	Poor	Score
Part D **Ethical evaluation** **(25%)**	Able to provide an apparent and reasonable assessment of ethical issues raised from the chosen topic. Excellent justification on such ethical issues with well appropriate selection of the ethics philosophy to support it. Able to give excellent interpretations and consider numerous views from related perspectives based on facts, rules, and laws relevant to the ethical problem. **(21 - 25%)**	Able to provide a clear and reasonable assessment of ethical issues raised from the chosen topic. Reasonable justification on such ethical issues with well appropriate selection of the ethics philosophy to support it. However, some explanations are not clear. Able to verify whether the facts are relevant or not based on facts, rules and laws relevant to the ethical problem. **(16 - 20%)**	Average to provide a clear and reasonable assessment of ethical issues raised from the chosen topic. Average justification on such ethical issues with a little point to support it. Able to gather facts related to ethics problems but some of it is irrelevant. **(11 - 15%)**	Poor to provide a clear and reasonable assessment of ethical issues raised from the chosen topic. Insufficient justification on such ethical issues with very limited or no point to support it. **(1 - 10%)**	

TOTAL MARK: /100

Lecturer/Tutor's Feedbacks/Comments:

Acknowledgement

We are really grateful because we managed to do our Social and professional issues assignment within the time given by our lecturer, Ms. Lim Siew Moi. She shared many things such as her experience for us to increase our knowledge. This assignment cannot be done without the effort and cooperation from our group members. We also sincerely thank Ms. Premawati for the guidance and encouragement in finishing the assignment and also for teaching us in this course. Last but not least, we would like to express our gratitude to our friends and classmates for their support and willingness to spend some time with us on this project.

Table of contents

1.0 Background **1**

2.0 Analysis - Case Studies **2**

2.2 Legal 4

2.3 Architecture 4

2.4 Market perspectives 6

3.0 Solutions **8**

3.1 Social 8

3.2 Legal Law 8

3.3 Architecture 9

3.4 Market 10

4.0 Ethical evaluation **12**

5.0 Summary **13**

Reference **14**

Appendix **17**

1.0 Background

As the technology is rapidly developing in Malaysia, it has brought us more opportunities and more new applications. In the past few years, people have started using the internet for illegal purposes. It is called cybercrime which may cause an immeasurable loss to the person , company or the government. They usually carry out cybercrime by using a computer and network to generate profit from it. (Brush & guide, 2021) There are different types of cybercrimes like DDOS Attacks, Botnet, Malware, Phishing scams and more. All these will ruin the person's lives and the people who are involved or do attack are called hackers. On an individual level, many people affected by this issue have committed suicide. The ultimate loss is the person who is left helpless and left with no choice but to take extreme measures. As for the company, it causes a loss when they are forced to pay the criminals for the data they stole. The common cases that will be seen are the cybercrimes targeting the government. This can lead to the leakage of sensitive data, which could affect the nation's sovereignty. These issues can cost the government a huge sum of money. (Farhana Sheikh Yahya, 2020)

The cybercrime cases have risen much more during the COVID-pandemic. This is because criminals are taking use of the Internet to defraud individuals, especially during the Movement Control Order (MCO). Cybercrime is a sort of criminal behaviour that primarily involves the use of computers and networks as a medium target. Any internet user can be affected, and anyone with a work computer and Internet access can potentially become a cybercriminal. Some people lose their jobs during this pandemic and need money to survive. It is obvious that this is one of the reasons for them to take advantage to earn money. According to statistics by Malaysia Computer Emergency Response Team (MYCERT), from January to October 2021, there have already been 8922 reported cybercrime incidents this year. The reported cybercrime incidents include malicious codes, vulnerabilities report, Denial of Service, intrusion attempt, intrusion, fraud, content related, cyber harassment and spam. (Star, 2021)

There are many general stakeholders involved in cybercrimes. For example, the hackers, the people who are affected by the fraud, the police who investigate the cybercrime case and the legal authorities who prosecute the cybercriminals. These stakeholders have different roles in the occurrence of cybercrime. The Malaysian government is the main player in cybercrime cases. Malaysia has been taking measures to prevent cybercrime cases from taking place. The ministry of home affairs, the Ministry of Communications and Multimedia, and the Malaysian Communications and Multimedia Commision (MCMC) have been actively involved in cybercrime prevention. To prevent cybercrime cases, the government has given priority to educating the internet users. (Khaniejo, n.d.)

2.0 Analysis - Case Studies

There was a cybercrime incident about the fraud that happened to a 74-year-old Petaling Jaya woman. This elderly woman received a call from a person claiming to be from PosLaju Malaysia headquarters. She was informed that they were holding a package containing an Identification Card (IC), a cheque book, and three bank cards in her name. After that, the phone call was then transferred to an individual named "Siwan", purportedly from Sabah Contingent Police Headquarters, stating that she was engaged in a money laundering case and is under investigation. The victim was threatened with arrest and custody if she failed to assist the police during their investigation. The victim was terrified so she followed the fraudster's commands and gave the scammer her bank account details and transferred RM833,000 from her Tabung Haji account into another Maybank account belonging to her. After that, she was told to transfer RM159,000 to other bank accounts in a series of transactions. After a period of time, the victim recognized that she had been duped and reported it to the police. The elderly victim had losses estimated at around RM1,007,673.33 to the Macau scammer. The syndicate frequently targets the elderly who lack awareness of cybercrime (Bernama, 2021).

Besides that, young women are vulnerable to cybercrime because they are readily influenced by social networking site features such as photo uploading. Most of the women like to publish images on social networking sites, which exposes them to the danger of cybercrime because anybody including criminals can access these pictures for numerous purposes. For example, cybercriminals will modify and transform the images into sexual photos in order to threaten, intimidate, or insult victims, putting pressure on them and causing them to make poor decisions (Ghani, Norhayati & Ghazali, Suriati, 2020). Some Telegram channels are particularly concerned with explicit content, publishing pictures of women in ordinary situations without their knowledge or agreement. Those pictures and videos are screenshots from their social media accounts, rather than being shared by the women themselves. Those telegram channels are essentially a group of people with thousands of members. They freely advertise and sell pictures of their ex-girlfriends, and they discuss and leak information about individual women. The young women victims will subsequently experience an influx of Instagram follower requests and harassment as a result of the image-based abuse. When such photos are shared and sent, the victims' physical and online safe will be threatened (Carvalho, 2021).

Moreover, there is another cybercrime case involving fake Bank Negara apps and websites. The police have warned the public that the MyBNM app is being exploited to perpetrate fraud by unscrupulous parties. The fake Bank Negara Malaysia apps recorded 105 cases with a total loss of RM4.8 million, while the website pretending to be Bank Negara Malaysia recorded 23 cases with a total loss of RM411,000. According to the pictures shared by the Royal Malaysia Police (PDRM), the fake Bank Negara Malaysia website will have links such as "www.bnm-govinfo.com", while the link to the real Bank Negara Malaysia website is "bnm.gov.my". A Twitter user with the name called azaliaspn asked Bank Negara Malaysia questions, stating that she had gotten a call from Bank Negara Malaysia requesting that her bank accounts be protected. She was then given a website to use to execute the operation, which was named myBNM. According to Bank Negara Malaysia, which stated that the call was an impersonation fraud and mentioned that Bank Negara Malaysia would never call users about their bank account. Also, there was another victim who was encouraged to enter his personal financial information into a fake Bank Negara Malaysia website, then he lost RM33,000 in total. According to an article in Sinar Harian, scammers would pretend to be police or bank officers.

Victims will be prompted to download a fake Bank Negara Malaysia app or log in to a website to fill in their bank data as part of a procedure to ‘resolve’ a banking issue. The National Cyber Security Agency (NACSA) has posted an alert to warn how scammers can get access to victims’ online bank accounts by convincing them to download a malicious app bearing Bank Negara Malaysia's logo. The Royal Malaysia Police (PDRM) has asked the public to check the features of any mobile application or websites that resemble banking, judiciary, or enforcement authorities (Yeoh, 2020).

2.1 Social

The social impact of cybercrime refers to social damage and other aspects. People are growing increasingly reliant on digital technology as science and technology advance, which has resulted in an increase in cybercrime. It brings a wide range of problems to people’s daily life, as well as a wider range of worries, such as worry or lack of confidence in the Internet or technology. Cybercriminals use cybercrime to steal money and identities from individuals. As the case above, the 76 years old woman got scammed over RM1 million from the fraud. This impacts the society of being flustered because they need to be aware to transfer money to people. This kind of fraud will spread worldwide, not only happening to the old lady but many people out there who have been scammed with the same method too. Fraudsters might take out loans, solicit debts, accumulate debts, and then escape. Rehabilitating a victim’s identity might take years. Therefore, money, safety, and peace of the society will be destroyed too.

Another example would be that previous victims of social harassment and computer abuse could take precautions to prevent becoming a victim again in the future. The great majority of the victims have only been harmed once, with only a tiny percentage claiming to have been harmed twice or more. There are statistics to back up these assertions, suggesting that when users become victims of internet crime, they are fast to learn from their mistakes. For instance, women experienced sexual harassment while using social media. Sexual harassment is evident when it comes to praising a woman’s body and discussing sex. This harassment frightens the victim and forces them to make their account private and filter followers after being harassed. In addition, victims are also less likely to post pictures of themselves on social media if they have previously been harassed. This incident shows that through the use of social media applications, young women are vulnerable to cybercrime risks.

Individuals who believe they are capable of managing prospective hazards may not be afraid or avoid threats. People who believe they are ineffectual in exerting control over possible risks, on the other hand, respond with tension and avoid having any interaction with them, therefore avoiding them. For example, in the event of a cyber-related occurrence such as a phishing scam, individuals may perceive themselves as lacking the requisite skills or knowledge to avoid such an incident, preventing them from acting or taking preventative measures. If this happens on a wide scale, it may have a significant social impact. As the case above is about a phishing attack and it is the most common scam on the Internet. The criminal using the fake account of Bank Negara Malaysia asks the victims to download the malware app just to steal the victim’s sensitive information such as usernames, passwords, and financial information. Hence, this will let the public lose their faith and trust in these malware applications. The reason is that they might have a stereotype of the website or applications trying to collect their privacy and sensitive information and steal their money out of nowhere. For instance, the criminal led the victim to download the “Bank Negara Malaysia” malware application and stole his money inside his bank account. This might lead the victim to be afraid to download any banking application and do online transactions in the future.

2.2 Legal

There are many cyber crimes in Malaysia, causing many people to be harmed, and cybercrime cases may occur because of loopholes in Malaysia's existing relevant laws and regulations. As there are many cybercrime cases, and there will be new criminal methods, the regulations of the law have not been able to increase and solve the loopholes in the cybercrime law in a timely manner. According to the case above, the laws cannot support the fact that the old lady is being deceived, because the law does not record detailed punishment, so criminals cannot be convicted. Criminals will discover this and commit crimes to defraud property. Loophole laws cannot protect victims from fraud, because fraudsters may disable their phone numbers after committing a crime. This resulted in the police being unable to track the fraudulent phone number to find the identity of the fraudster. As a result, the law cannot bring them to justice and cannot protect the victims from fraud.

Cybercrime has attracted much attention in Malaysia, and people will also use social media with the technology of the times to facilitate communication with friends from far away. This is also a good way to connect with friends and share their lives on social media. Friends can feel at ease when they see it, but this criminal uses cybercrime tactics to harass people and stalk them. This also has a serious impact on the law by not cracking down on cyber crimes**,** making them more aggressive in committing crimes to harm the people. In the second case, criminals targeted young women because they liked to harass beautiful girls and track them to achieve their goals, such as intimidation. Although there is a law in Section 233, Communications and Multimedia Act 1998 (Improper use of network facilities or network services) which can accuse criminals of harassing female users or explicitly protect female users. However, young women do not believe in the law, and they choose to remain silent because they find it embarrassing to report. This will make criminals more and more arrogantly harass young women who dare not stand up for themselves.

In the case of cybercrime, many people are beginning to be deceived, and criminals will use new methods to defraud other people's property. There was an impact because law enforcement and judicial institutions have no deterrent. Criminals will ignore the existence of the law and commit crimes. For example, criminals can forge property identities and invade victims' accounts to commit crimes. In the cybercrime case involving fake National Bank applications and websites, scammers would pretend to be police officers or bank officials. Victims will be prompted to download a fake Bank Negara Malaysia app or log in to the website to fill in their personal data and they think the problem has been solved, but they actually fell into a trap. The law has limited law enforcement and judicial institutions therefore, cybercrime cases are getting more and more serious. As a result of this circumstance, the use of phishing has grown ubiquitous, allowing criminals to operate freely and without fear of being prosecuted because there is no deterrence from law enforcement and legal authorities.

2.3 Architecture

In the modern development of technology, people rely more on the architecture of hardware and software technologies. Therefore, people's information is extremely vulnerable and may be accessed from any source. People usually prefer to use free services instead of paying. However, before users can use the "free" service, many web-based services will ask users to register by

providing names, phone numbers, email addresses, and other information. Some malicious people will make this part of their business goal by selling the data they collect. According to the case above, the elderly woman received a phone scam call from a fraudster and lost around RM1 million. The fraudster may have purchased a list of information from the web-based service and directly called the victim one by one, publishing the victims' names and information provided by the "free" web-based service, and letting the victim believe their words. This is their trick to let victims fall into their trap and pay them willingly.

From the architecture perspective, threats can be translated from the internet into offline harms due to cybercrime. Online threats can be translated into offline harms due to online crime. When we connect our lives to the Internet, it is easy to be threatened by criminals. This makes the threat of cybercrime more dangerous. In the second case, the woman who always posts pictures on social media and the criminals doctored her picture into a pornographic photo. Then, criminals will use these photos and her phone number to offer inappropriate sex offers to others to earn money. Other than that, criminals threaten, intimidate, or insult women, put pressure on them, and cause them to make wrong decisions. This has caused threats to her private life and shows the blurred border between the real world and the internet. Female users are relatively timid, they will easily get affected by these incidents.

Users of all technologies and systems usually are the weakest link in the safety chain system due to a lack of technical understanding. This is because people do not grasp the product's flaws they are dealing with, cybercrime risks like social engineering and carding become more common. Nowadays, phishing fraud is one of the most frequent cases reported in Malaysia. Social engineering techniques are well in use in phishing attacks to redirect users from original websites to malicious websites. Based on the case above about a phishing attack, the lack of anti-phishing software is one of the reasons that bring a negative impact on architecture. As the victims got scammed because they did not notice that they were on the fake website. The fake websites have similar website links, logo design, and operation design. This would confuse the victims who are not familiar with the Internet web pages. The fake Bank Negara Malaysia website would have links like "www.bnm-govinfo.com", while the real bank Negara Malaysia website would have links like "bnm.gov". If anti-phishing software is installed, users will be warned when they enter the phishing website. The trick was that the people got a call from Bank Negara Malaysia asking to protect their bank account. They then get a website to perform the operation, called myBNM. According to Bank Negara Malaysia, the call was a fake fraud and mentioned that The bank would never call users to ask about their bank account. Criminals were encouraged to enter their personal financial information into a fake Bank Negara Malaysia website that cost them a fortune.

2.4 Market perspectives

People often use the Internet for money transactions as it is really convenient and hackers take these opportunities to commit cybercrimes to earn money. They first collect information on their targeted target. Most of them are wealthy and less intelligent technology users. As cybercrime cases are getting serious, the older generation will not trust the Internet. This might affect the online market in this modern crisis. They are not familiar with all these new technologies and this will give such a big advantage to the hackers. This will leave a psychological shadow on the elderly, they will begin to distrust the Internet, and they will begin to deceive. In the first case, the fraudster disguised his identity and threatened to make the elderly woman follow his instruction. The fraudster tells the stories seriously and causes the elderly woman to be tenser

and more easily fall into the trap. After the elderly woman believed the fraudster, he then instigated step by step to ask the elderly woman to do online transactions. As a result, this incident causes them to not believe the Internet easily, which may put the market into a crisis and makes the market into a crisis. People are wary of the Internet, and they can choose to block strangers from unknown sources.

Modern Internet platforms are very extensive, and many people will download and use them, such as Telegram, Facebook, Instagram, etc. People share their lives on social media, and cybercrimes can also be committed through social media. This also reduces the use of social media in the online market and also affects the income of social media. For developers of social media, they develop various social media not only for the convenience of people but also to make money, which also gives criminals opportunities. Criminals on the Internet have begun to harass and stalk women, which has led to a significant decrease in women who use social media in the online market, reducing the number of users. Based on the cybercrime case above, the cybercriminals will modify the young women's pictures to make them into sexual images in order to threaten, harass, or insult the victim and exert pressure on them. Hence, this led to the young women victim making poor judgment and following the instructions of the cybercriminals to do something bad. The young women victims may have a bad impression of social media and are afraid of using it, resulting in a significant drop in profit and credibility of the social media.

With the improvement of the present-day internet, it's very broad, and many humans will use the Internet for his or her convenience. Online banking on the Internet is very convenient to use. We do not need to go to the bank purposely to process our needs. For example, transfer, save money, pay insurance, pay bills, and so on. However, this also allowed criminals to conduct new crimes and affected Malaysia’s online banking into a crisis, leading to a decline in the reputation of Malaysia’s online banking. People must beware and understand the deceptions of criminals to prevent criminals from harming people. In the third case, the criminal would claim to be Bank Negara Malaysia, the call was a fake fraud and mentioned that Bank Negara Malaysia would never call users to ask about their bank accounts. In addition, another victim was encouraged to enter his personal financial information into a fake Bank Negara Malaysia website, he then lost a total of RM33,000. Criminals will convince people to use their bank website by telling lies. The people who are easy to deceive will take photos of their ID cards and send them to him to check the problem. Criminals will use their ID cards to commit crimes. The people who have been cheated and lost an amount will no longer use online banking as they do not trust the bank anymore. This brings disadvantages to the bank as the citizens no longer support them and their revenue is decreased.

3.0 Solutions

3.1 Social

Update internet knowledge. Nowadays, most of the old generations do not have internet knowledge, but they are forced to use the internet in their life. This is because they need to follow the new era to communicate with society. As previously stated, the 76-year-old woman was defrauded by almost RM1 million by cybercrime. Therefore, adults should talk to the older generations about internet knowledge. Without cutting off the communication channels, they must teach them how to use the internet in a responsible manner. If they are being harassed, stalked, fraud, or bullied online, they will know the way to solve it such as seeking help from police or family, and will not follow the instructions of the cyber criminals without thinking. Because of doing that, their attitude or behaviors can be more confident in terms of using the online platform.

Nowadays, people are afraid of using online platforms because their information is vulnerable to malicious people. Therefore, parents should educate their children by not posting or sharing sensitive photos on social media. Social media now allows people to set their accounts as private. Social media users should only show their profiles to their close friends and families. Parents should protect their children who are under 18 from identity theft. Children under 18 are usually targeted because they are still new to society. The parents should guard their children while they share their personal information. Let them know the impact that will bring to them and brainwash them with the awareness of cybercrime.

People should know that identity crime or theft can occur anywhere. It is important to know how to protect their identity such as private information or bank account anytime and anywhere. There are various approaches that people can take to help prevent criminals from obtaining their private information. People should not reply to phishing emails or short-message-service (SMS) even though someone asks you to do so, because you never know if the message is reliable. Besides that, people must suft wisely on the websites. A TRUSTe “Trustmark” is important to check on every website. This certified the original website's owner who had followed their private policy.

3.2 Legal Law

Due to the fact that cybercrime laws in Malaysia have loopholes, they should update the laws to fight against cybercrime such as the Computer Misuse Act (CMA), Computer Fraud & Abuse Act (CFAA). The law is known as cyberlaw, and it will help in the coverage of all connected aspects of transactions and activities which apply to the internet or cyberspace. There are some legal aspects for every reaction and action that occurs in cyberspace. The cybercriminals' tactics can be in various ways so the cyber law should be updated from time to time. Although the current number of cybercrimes in Malaysia increases, the updated laws will assist to define the level of current and accepted behaviors for the users who access information and communication technology. Besides, it assists to create socio-legal sanctions effectively for cybercrime; protecting humans who use online platforms. Generally, it mitigates and prevents causing harm to people, data and system, infrastructure, and services. It helps to give protection to human rights and allows the investigation and prosecution of those crimes that are committed online. (Cybercrime Module 3 Key Issues: The Role of Cybercrime Law, 2021)

Nowadays, the Internet has become a big aspect of everyone's lives, especially youngsters. It provides a great opportunity for all the citizens, especially young ladies, to learn and understand how the legal laws fight against cybercrime. Even mature, intellectual, and tech-savvy adults, sometimes may be the victim of cybercrime. We can confirm that a person full of curiosity but lacking in maturity and knowledge can become the target of cybercrime. Therefore, it is important for the government to allow its citizens to understand how legal law fights against cybercrime. It is also helpful if their teachers get involved in this conversation. For example, the government can arrange teenagers to have classes in their studies so that the teachers can incorporate some knowledge of cyber security and cyber laws during their lessons. When someone is facing cybercrime, they will know how to use legal ways to bring the cybercriminals to justice and the citizens, especially young ladies, would not easily fall into wrong hands again. Therefore, the victims of cybercrime especially young ladies will be reduced.

Offer strict punishment to cybercriminals. The Computer Crimes Act 1997 (CCA) which is the cybercrime law in Malaysia, still cannot control the risk of cybercrime. The current penalties for a convicted offense are from RM25,000 to RM150,000 or imprisonment for three to ten years, or both, depending on the type of cybercrime offense committed. However, those laws still cannot deal with cybercriminals because they will take legal loopholes to escape. Therefore, strict laws are needed to implement to fight against cybercrime. For example, it should increase the amount of penalty or the period of imprisonment. Therefore, people will have more concerned about cybercrime and will not get involved in cybercrime.

3.3 Architecture

Apply the phone application which supports the security. This is important to make it because the case of cybercrime is increasing especially during the covid-19 pandemic and the old folks are always the fraud victim. Therefore, it should carry out some applications that can determine the “fake calls” apps such as Truecaller. Truecaller normally is an application that can determine who is making a call with you. Telemarketers, spam calls, and especially fraudsters can all be blocked with the assistance of this type of caller identification. Truecaller applies the contact details that come from the provider of the network, and the data from another user to group the callers into Safe or Spam callers. Users can know whether it is spam or not with the color of incoming calls. A red contact card indicates that users should avoid accepting the call while a blue contact card shows that it is safe to pick up. Therefore, it is useful for the old folks because they can differentiate the color in order to prevent fraud cases.

Don’t overlook safeguarding personal hardware and software. Becoming the victim of cybercrime is frequently caused by the security of hardware and software is bad, therefore securing their hardware is a simple technique for boosting your cyber security. The firewall cannot completely guarantee that all other aspects of protection are covered but people can update and safeguard their personal hardware and software manually. For example, people can set the settings of their hardware to avoid their media or pictures will not being viewed by third parties in social media software. People are also prevented from posting personal or sensitive information on any social media platform with weak security personal hardware. Next, people can implement security software in their hardware that can block cybercriminals from stealing their photos. Hence, people should always check and update their security software and hardware from time to time.

Must keep applying the software which assists to differentiate between the original and fake websites in order to prevent cybercrime such as the fraudster sending the fake link to the victims, and they undergo cybercrime in the fake websites. For example, it is beneficial for people to

implement Kaspersky VirusDesk in their devices. Kaspersky is a recognized security solution vendor with a 30-year track record of success. It includes the features which are the virus scanner and fake website checker. The user only needs to paste the domain address in questions and receive the response in a short period. Besides, users can drag and drop the files that are suspicious to examine for risk software. Kaspersky VirusDesk acts as a tool to examine the reputation of a website and can present to users whether the link is safe or not. Other than that, the tool of Kaspersky knows that the advertisements can bombard the users against their view. Therefore, this is the reason why the URLs contain many spam and pop-ups. Then, the checker of the website will also notify the users if there is no data available in the portal. It depends on the user whether to visit the website if it is worth a risk.

3.4 Market

Update cyber security of online markets from time to time. It will help the bank to prevent adware. For instance, adware is a type of computer virus that automatically shows or downloads advertising content such as banners or pop-ups while a user is online. These advertisements will entice people to click on them when making transactions at an order, allowing the other malware to access your device. Cybercrime will start to hack the system of the bank. People are often using online banking to make payments in the online market. Therefore, these problems will be solved by updating cyber security and allowing people to bring back confidence towards banks in order to continue purchasing at online platforms.

Nowadays, businesses can be operated on social media platforms such as Facebook and Instagram. Cybercrime may bring negative effects to online businesses such as they will steal customer or vendor information or media. To prevent this, businesses can utilize a virtual private network (VPN) to gain access to online business platforms when promoting and advertising their products or services more safely and effectively. For example, whenever a consumer expresses an interest in a product, the online platform will recommend and display relevant products and services to the customer. If the product is acceptable to customers, then the transaction will be undergone. The information of customers and vendors will be secured with the use of a VPN. People will feel more confident to make purchases on online platforms. Hence, it will not affect the revenue of the online business negatively.

Nowadays, the marketplace conducted online is known as e-commerce and people are preferring to use online banking to make transactions on this platform. Implementing cyber security such as antivirus in the device will protect the bank while users make transactions. For example, the antivirus will include comprehensive digital protection such as technical security attacks. It also offers a lot of features which are firewall booster, layered ransomware protections, and Pay Guard browser which offer the protection most trustworthy levels against online banking. The information of the users such as name, phone number, and id number will be secured. Therefore, cybercriminals cannot get their information to commit cybercrimes. It will help the customers to save money by preventing them from being subjected to potential threats when assessing online banking.

The latest bank website has offered basic yet effective security advice, advertisements, and information in order to assist people to become more aware and security-conscious users. For example, the public bank official website, it more considers the security of the internet and online banking of their users. Therefore, users will understand the current security threat before making any transactions. Users can understand it more by accessing the online security page which is available on the public bank official website and there will provide a lot of information such as Commercial Crime Prevention Campaign (Online Crime) 2021, types of threats, scam

awareness video, and so on. It had provided the information to identify fake websites. For instance, the real website will show a padlock symbol to define it as a secured website. Hence, people will more understand the bank is committed to delivering high levels of online security and secrecy to provide them with complete peace of mind when using its service. Therefore, people will obtain knowledge of cyber security which can avoid cybercrime in order to re-establish trust in the bank.

4.0 Ethical evaluation

Based on the first case study which is about the 74-year-old woman who encountered a cybercrime incident that required her to transfer money to an unknown bank account which is controlled by the scammer, the ethical act that the woman is performing is **act utilitarianism**. This is because the elderly woman was actually afraid of what is happening to her and she does not know what is actually happening, so she decided to follow the commands given by the Macau scammer who pretended to be Sabah Contingent Police Headquarters. The elderly woman only focused on the consequences as the scammer frightened her that she was engaged in a money laundering case and she was threatened with arrest and custody if she failed to assist and collaborate with the "Sabah Contingent Police Headquarters". This is because when the woman performs this ethical act, the affected party which is the scammer will be gaining benefits from the woman while the woman will be suffering from the fraud.

Based on the second case study which is about the young women who are involved in cybercrime which their images will be edited and transformed into sexual photos and threatened by the scammer for purposes. The ethical act that the young women are performing is **ethical egoism**. This is because the Internet, such as social media, is a public platform that allows everyone to post their comments and pictures in order to share their happiness together. The young women are doing good because they are focused exclusively on their self-interest which is sharing their comments or pictures online. However, there were some immoral people take the opportunity to download or retrieve the photos of the young women without their consent and tried to edit their photos and convert into sexual photos and threaten them. The cybercriminals are performing **Kantianism** as an ethical act due to they are using other people solely to gain benefits from what they did such as threatening the young women by editing their photos into sexual photos. According to news that happened last year, a South Korean citizen which is the leader of an online sexual blackmail ring that always targeted young women was sentenced to 40 years in jail. He tried to host online chat rooms on Telegram where users paid to see young girls performing sexual acts while the leader tried to blackmail the young women to upload explicit images onto the chat rooms in order to allow the users to satisfy themselves as they have been paid. (Jessie Yeung and Yoonjung Seo, 2021)

Based on the third case study which is about the cybercrime case involving the fake Bank Negara applications and websites, the ethical act that the police was performing in the case is **rule utilitarianism**. This is because the police have warned the public that the MyBNM application is a fake application that is being exploited to perpetrate fraud by unknown parties or scammers. They have done their job of spreading warning messages to the public and hope the public will beware. However, there are still victims suffering or countering from the fraud as they did not read the warning messages that were published by the police. People need to always have a look or check on the police updates in order to know what is happening in society nowadays. Although if the matter rarely happens to the others, they also need to get to know what is happening in order to forward the warning to the friends and families to prevent our beloved friends and family members from encountering this kind of fraud.

5.0 Summary

Cybercrimes are a type of criminal behavior that mainly involves the use of computers and the Internet which may cause an immeasurable loss to the person, company, or the government. The ultimate loss will cause the person only left helpless and left with no choice. All these will ruin the person's lives and the people who are involved or doing attacks are called hackers. The reported cybercrime incidents include malicious codes, vulnerabilities reports, Denial of Service, intrusion attempt, intrusion, fraud, content-related, cyber harassment, and spam. Cybercrime is a sort of criminal behavior that primarily involves the use of computers and networks as a medium target. There are many general stakeholders involved in cybercrimes. These stakeholders have different roles in the occurrence of cybercrime. Malaysia has been taking measures to prevent cybercrime cases from taking place. The ministry of home affairs, the Ministry of Communications and Multimedia, and the Malaysian Communications and Multimedia Commission have been actively involved in cybercrime prevention.

There was a case in which an elderly woman had losses estimated at around 1 million to the Macau scammer, due to her lack of awareness of cybercrime. She was threatened with arrest and custody if she failed to assist the police during their investigation. Due to her timid, terrified and lack of internet knowledge, she can just follow the fraudster's commands and slowly fall into the trap. This kind of fraud will spread worldwide, not only happening to the old lady but many people out there who have been scammed with the same method. As the fraudulent IP address is hard to be identified, the police and law cannot bring them to justice and cannot protect the victims from fraud. This will leave a psychological shadow on the elderly, they will begin to distrust the Internet, and they will begin to deceive. Therefore, the elderly should always update their internet knowledge. The younger generation should share the awareness with their elderly to prevent fraud. The government should also update the cyberlaw so it would help in the coverage of all connected aspects of transactions and activities which apply to the internet. The other way to prevent fraud is to use a phone application like "Truecaller" which may help them to identify unknown calls and also block spam calls.

Developers of social media develop various social media platforms not only for the convenience of people but also to make money, which also gives criminals opportunities. There was a young women's picture that has been modified into a sexual photo and spread around on the internet. This called sexual harassment and which may cause young women less likely to post pictures of themselves on social media. They even feel embarrassed to report and remain silent, because their timid criminals are taking advantage and are not afraid of the law. Other than that, criminals threaten, intimidate, or insult women, put pressure on them, and cause them to make wrong decisions. This has caused threats to her private life and shows the blurred border between the real world and the internet and resulting in a significant drop in profit and credibility of social media. Therefore, parents should guard their children while they share their personal information. Let them know the impact that will bring to them and brainwash them with the awareness of cybercrime. Government should also spread the information to let the citizens understand how legal law fights against cybercrime and bring criminals to justice. Citizens should also protect themselves by protecting their devices, avoiding posting sensitive pictures, or set them as private so it is not being viewed by strangers.

Online transactions are one of the common ways that people use to transfer money, but scammers take this opportunity to make money. There was a case in which scammers pretend to be police or bank officers to prompt victims to download a fake Bank Negara app or log in to a

fake website to fill in their bank data. The law has limited law enforcement and judicial institutions therefore, cybercrime cases are getting more and more serious. Other than that, the victims will not notice that they were on the fake websites as they just look really similar. Hence, this will let the public lose their faith and trust in these malware applications. The people who have been cheated and lost an amount will no longer use online banking as they do not trust the bank anymore. This brings disadvantages to the bank as the citizens no longer support them and their revenue is decreased. Therefore, people should not reply to phishing emails or short-message-service (SMS) even though someone asks you to do so, because you never know if the message is reliable. They should install Kaspersky VirusDesk on their device. A TRUSTe "Trustmark" is also important to check on every website they browse. Strict laws should be improved to fight against cybercrime. Banks should also show a padlock symbol to define as a secured website so that people can easily avoid cybercrime.

The ethical evaluation of the first case study which is about the 74-year-old woman who encountered a cybercrime incident that required her to transfer money to an unknown bank account which is controlled by the scammer is the ethical act that the woman is performing is act utilitarianism. In the second case, the cybercriminals are performing Kantianism as an ethical act due to they are using other people solely to gain benefits from what they did such as threatening the young women by editing their photos into sexual photos. He tried to host online chat rooms on Telegram where users paid to see young girls performing sexual acts while the leader tried to blackmail the young women to upload explicit images onto the chat rooms in order to allow the users to satisfy themselves as they have been paid.

References

Brush, K., 2021. *What is cybercrime? Definition from SearchSecurity*. [online] SearchSecurity. Available at: <https://searchsecurity.techtarget.com/definition/cybercrime> [Accessed 17 November 2021].

Carvalho, 2021. *Abuse and anger: inside the online groups spreading stolen, sexual images of women and children*. [online] The Star. Available at: <https://www.thestar.com.my/aseanplus/aseanplus-news/2021/06/07/abuse-and-anger-inside-the-online-groups-spreading-stolen-sexual-images-of-women-and-children> [Accessed 26 November 2021].

Chia, Lee & Associates. (2021). Basics of Cyber Security Law in Malaysia. [online] Available at: https://chialee.com.my/basics-of-cyber-security-law-in-malaysia/. [Accessed 26 November 2021].

Cybercrimejournal.com. 2021. [online] Available at: <https://www.cybercrimejournal.com/Jiow2013janijcc.pdf> [Accessed 17 November 2021].

Unodc.org. 2021. *Cybercrime Module 3 Key Issues: The Role of Cybercrime Law*. [online] Available at: <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html> [Accessed 26 November 2021].

Farhana Sheikh Yahya, S., 2021. [online] Astroawani.com. Available at: <https://www.astroawani.com/berita-malaysia/rise-cybercrime-malaysia-what-you-need-avoid-264890> [Accessed 17 November 2021].

Ghani, Norhayati & Ghazali, Suriati, 2020. *The Vulnerability of young women to cybercrime : A case study in penang.* [online] researchGate.com Available at :

<https://www.researchgate.net/publication/348230968_THE_VULNERABILITY_OF_YOUNG_WOMEN_TO_CYBERCRIME_A_CASE_STUDY_IN_PENANG_European_Proceedings_of_Social_and_Behavioural_Sciences_EpSBS> [Accessed 19 November 2021].

Jessie Yeung and Yoonjung Seo, C., 2021. *Leader of South Korean sexual blackmail ring sentenced to 40 years*. [online] CNN. Available at: <https://edition.cnn.com/2020/11/25/asia/korea-telegram-sex-crime-verdict-intl-hnk/index.html> [Accessed 29 December 2021].

Khaniejo, N., 2021. [online] Cis-india.org. Available at: <https://cis-india.org/internet-governance/files/economics-of-cyber-security-part-ii> [Accessed 17 November 2021].

Mycert.org.my. 2021. *MyCERT : Incident Statistics - Reported Incidents based on General Incident Classification Statistics 2021*. [online] Available at: <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=ed7db903-3550-489d-beaf-66bd25de4d4b> [Accessed 2 December 2021].

Norton.com. (2018). Norton. [online] Available at: https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. [Accessed 2 December 2021].

NST Online. 2021. *74-year-old PJ woman loses RM1 million to Macau scam syndicate | New Straits Times*. [online] Available at: <https://www.nst.com.my/news/crime-courts/2021/02/663224/74-year-old-pj-woman-loses-rm1-million-macau-scam-syndicate> [Accessed 17 November 2021].

Star, T., 2021. *Protection against cyber crime | Malaysian Communications And Multimedia Commission (MCMC)*. [online] Malaysian Communications And Multimedia

Commission (MCMC) | Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Available at: <https://www.mcmc.gov.my/en/media/press-clippings/protection-against-cyber-crime> [Accessed 17 November 2021].

www.truecaller.com. (n.d.). Truecaller is the leading global platform for verifying contacts and blocking unwanted communication. | Truecaller. [online] Available at: https://www.truecaller.com/ [Accessed 25 November. 2021].

www.pbebank.com. (n.d.). PBe Online Security. [online] Available at: https://www.pbebank.com/onlinesecurity/index.html. [Accessed 24 November. 2021]

Yeoh, A., 2021. *PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil in losses*. [online] The Star. Available at: <https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses> [Accessed 25 November 2021].

Appendices

Originality report

COURSE NAME
202109 BACS3033 (T)

STUDENT NAME
ZHI YING SOH

FILE NAME
SPI Assignment (due 4 DEC)

REPORT CREATED
Dec 4, 2021

Summary

Flagged passages	13	3%
Cited/quoted passages	3	0.4%

Web matches

thestar.com.my	5	1%
nst.com.my	2	0.5%
nestia.com	2	0.4%
cnn.com	1	0.3%
mcmc.gov.my	2	0.2%
rajahtannasia.com	1	0.2%
lowyat.net	1	0.1%
business.site	1	0.1%
unodc.org	1	0.1%

1 of 16 passages

Student passage CITED

...reported cybercrime incidents include malicious codes, vulnerabilities report, Denial **of** Service, intrusion attempt, **intrusion**, fraud, **content related, cyber harassment** and **spam**. (Star, 2021)

Top web match

Fadillah said most **of** the cyber crime cases received by Cyber999 involved **intrusion, content- related, cyber harassment**, denial of service, **spam**, fraud, intrusion attempt, malicious codes and...

Protection against cyber crime - Malaysian Communications And ... https://www.mcmc.gov.my/en/media/press-clippings/protection-against-cyber-crime

2 of 16 passages

Appendix i : Originality Report pg1

Student passage FLAGGED

...happened to a 74-year-old Petaling Jaya woman. This elderly **woman received a call from a person claiming to be from PosLaju** Malaysia **headquarters**. She was informed that they were holding a package...

Top web match

... Mohd Faisal said the 74-year-old **woman** claimed she had **received a call from a person claiming to be from PosLaju** Malaysia's **headquarters** on Sept 25.

Retiree, 74, taken for a million-ringgit ride - Lowyat Forum https://forum.lowyat.net/topic/5098492

---

3 of 16 passages

Student passage FLAGGED

...to be from PosLaju Malaysia headquarters. She was informed **that they were holding a package containing an Identification Card (IC), a cheque book, and three bank cards** in **her name**

Top web match

The elderly woman received a call on Sept 25 last year, purportedly from Pos Malaysia headquarters saying **that they were holding a package containing an Identification Card (IC), a cheque book, and**...

74-year-old PJ woman loses RM1 million to Macau scam syndicate https://www.nst.com.my/news/crime-courts/2021/02/663224/74-year-old-pj-woman-loses-rm1-million-macau-scam-syndicate

---

4 of 16 passages

Student passage FLAGGED

The victim was terrified so she followed **the** fraudster's commands **and gave** the scammer **her bank account** details **and transferred** RM833,000 **from her Tabung Haji account into** another **Maybank account**

Top web match

Frightened, **the victim** obeyed all orders by **the** scammers **and gave** away **her bank account** information to Si Wan, **and transferred** RM833,000 **from her Tabung Haji account into** her **Maybank account**,"...

74-year-old PJ woman loses RM1 million to Macau scam syndicate https://www.nst.com.my/news/crime-courts/2021/02/663224/74-year-old-pj-woman-loses-rm1-million-macau-scam-syndicate

---

5 of 16 passages

Student passage FLAGGED

A Twitter user with the name called **azaliaspn** asked Bank Negara Malaysia questions, stating **that she had** gotten **a call from** Bank Negara Malaysia requesting that **her bank accounts**

Top web match

On Nov 25, **a Twitter user with the** handle **azaliaspn** posed a question to BNM, claiming **that she had** received **a call from** BNM asking to protect **her bank accounts**.

PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil
... https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses

---

Appendix ii : Originality Report pg2

6 of 16 passages

Student passage FLAGGED

Victims will be prompted **to download a fake** Bank Negara Malaysia **app or log** in to **a website to fill in their bank** data **as part of a** procedure **to 'resolve' a banking issue**. **The National Cyber Security**...

Top web match

Victims will then **be** asked **to download a fake** BNM **app or log** into **a website to fill in their bank** details **as part of a** process **to 'resolve' a banking issue**...**The National Cyber Security Agency (NACSA)**...

PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil
... https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses

---

7 of 16 passages

Student passage CITED

...Bank Negara Malaysia's logo. The Royal Malaysia Police (PDRM) **has** asked **the public to** check **the** features **of any mobile** application **or websites** that resemble **banking, judiciary, or enforcement**

Top web match

PDRM **has** urged members of **the public to** carefully assess **the** details **of any mobile** apps **or websites** bearing similarities to **banking, judiciary or enforcement** agencies.

PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil
... https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses

---

8 of 16 passages

Student passage FLAGGED

Victims will be prompted **to download a fake** Bank Negara Malaysia **app or log** in to the **website to fill in their** personal data and they think the problem has been solved, but they actually fell into **a**

Top web match

Victims will then **be** asked **to download a fake** BNM **app or log** into a **website to fill in their** bank details as part of **a** process to 'resolve' a banking issue.

PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil
... https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses

---

9 of 16 passages

Student passage FLAGGED

...cybercrime; protecting humans who use online platforms. Generally, it **mitigates and prevents** causing **harm to people, data and** system, **infrastructure, and**

Top web match

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general,...

Appendix iii : Originality Report pg3

Cybercrime Module 3 Key Issues: The Role of Cybercrime Law https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html

---

10 of 16 passages

Student passage FLAGGED

...tech-savvy adults, sometimes may be the victim of cybercrime. **We can** confirm **that a** person **full of curiosity but** lacking **in maturity and** knowledge **can** become **the** target **of**

Top web match

And if mature, intelligent, sometimes even tech savvy adults can fall for scams online, **we can** be most certain **that a** child **full of curiosity, but** limited **in maturity and** awareness, **can** fall victim to...

Cyber Security Training Program with Thane City Police https://suyashcybersecurity.business.site/posts/2003529736007720753

---

11 of 16 passages

Student passage FLAGGED

...in Malaysia, still cannot control the risk of cybercrime. **The** current penalties **for a convicted** offense are **from RM25,000 to RM150,000 or imprisonment** for **three to** ten **years, or both**

Top web match

Depending on the type of offence committed, **the** fine **for a convicted** offence ranges **from RM25,000 to RM150,000 or imprisonment** of **three to** 10 **years or both**.

Cybersecurity 2019 - Rajah & Tann Asia https://www.rajahtannasia.com/media/3126/cyb19_chapter-21-malaysia.pdf

---

12 of 16 passages

Student passage FLAGGED

...photos. According to news that happened last year, a **South Korean** citizen which is the **leader of an online sexual blackmail ring that** always **targeted young women was sentenced to 40 years in jail**

Top web match

(CNN) The **South Korean leader of an online sexual blackmail ring that targeted** minors and **young women was sentenced to 40 years in jail** on Thursday, marking the end of an explosive criminal case that...

South Korean leader of online sexual blackmail ring sentenced to 40 ... https://edition.cnn.com/2020/11/25/asia/korea-telegram-sex-crime-verdict-intl-hnk/index.html

---

13 of 16 passages

Student passage CITED

...to 40 years in jail. He tried to host **online** chat **rooms on Telegram where users paid to see young girls** performing **sexual acts** while the leader tried **to**

Top web match

Appendix iv : Originality Report pg4

Cho Joo-bin, a 24-year-old man, hosted **online rooms on** encrypted messaging app **Telegram, where users paid to see young girls** perform demeaning **sexual acts** carried out under coercion, according **to**...

Dozens of young women in South Korea were allegedly forced into
... https://news.nestia.com/detail_share/3814821?media_type=1

---

14 of 16 passages
Student passage FLAGGED

...reported cybercrime incidents include malicious codes, vulnerabilities report, Denial **of** Service, intrusion attempt, **intrusion**, fraud, **content related, cyber harassment** and **spam**

Top web match

Fadillah said most **of** the cyber crime cases received by Cyber999 involved **intrusion, content- related, cyber harassment**, denial of service, **spam**, fraud, intrusion attempt, malicious codes and...

Protection against cyber crime - Malaysian Communications And
... https://www.mcmc.gov.my/en/media/press-clippings/protection-against-cyber-crime

---

15 of 16 passages
Student passage FLAGGED

...pretend to be police or bank officers to prompt **victims to download a fake** Bank Negara **app or** login to **a** fake **website to fill in their bank** data. The law has limited law enforcement and judicial...

Top web match

Victims will then be asked **to download a fake** BNM **app or** log into **a website to fill in their bank** details as part of a process to 'resolve' a banking issue.

PDRM: Fake Bank Negara apps and websites cost victims RM5.2mil
... https://www.thestar.com.my/tech/tech-news/2020/11/27/pdrm-fake-bank-negara-apps-and-websites-cost-victims-rm52mil-in-losses

---

16 of 16 passages
Student passage FLAGGED

...their photos into sexual photos. He tried to host **online** chat **rooms on Telegram where users paid to see young girls** performing **sexual acts** while the leader tried **to**

Top web match

Cho Joo-bin, a 24-year-old man, hosted **online rooms on** encrypted messaging app **Telegram, where users paid to see young girls** perform demeaning **sexual acts** carried out under coercion, according **to**...

Dozens of young women in South Korea were allegedly forced into
... https://news.nestia.com/detail_share/3814821?media_type=1

Appendix v : Originality Report pg5