Introduction:

Rachel:
Term *cyber* refers to anything that is related to computers, digital technology or internet. It encompasses online activities, virtual environment and electronic communication systems. Based on the description above, we can know what cybersecurity is. Cybersecurity is the pratice of protecting computer systems, networks and data from cyber threat such as hacking, malware and unauthorized access. It involves using technology, processes and best practices to safeguard sensitive information, ensure system integrity and prevent cyberattacks. Cybersecurity is essential for individuals, businesses and governments to protect against data breaches, identity theft and financial fraud.

Therefore, we will focus on Scam, which is a cybercrime. It is a fraudulent scheme designed to deceive people, usually for financial gain. Scammers will use manipulation, false promises and misleading information to trick victims into providing personal details, sending money or engaging in risky activities. Common types of scams include phishing emails, fake investment schemes, online shopping fraud and impersonation scams. Scams are a significant cybersecurity issue as they often exploit digital platforms and social engineering tactics to target victims.

Jia Wenbing:

The Internet is a virtual platform for information transmission, reception, and sharing. It connects information from various points, surfaces, and bodies, thereby realizing the sharing of these resources. The Internet is the most important invention in the history of human development, which has improved science and technology and the development of human society. The rapid development of the Internet has greatly facilitated people's lives, but it has also brought serious network security problems, especially the threat of Internet fraud. Internet fraud refers to illegal acts by criminals to defraud others of their property by fabricating facts or concealing the truth. There are endless fraud methods, including false shopping, impersonating acquaintances, impersonating customer service, investment and financial fraud, etc., which use the victim's trust or desire for cheapness to commit fraud, causing serious losses to individuals and society.

In order to prevent Internet fraud, we need to be vigilant and enhance safety awareness. Not trusting strangers' information, not clicking on unknown links or providing personal privacy data at will are the key to preventing being deceived. At the same time, using safe and reliable websites for transactions, regularly updating passwords, and learning relevant anti-fraud knowledge can effectively reduce the risk of being deceived.

Liu Ziyu:
A network is a graph composed of nodes and lines, which represents the objects of study and their connections. In mathematics, a network usually refers to a weighted graph, where nodes and lines can be given weights to quantify the closeness of the relationship between

nodes and the ease of information transmission. The physical meaning of a network is a model abstracted from practical problems, such as a switch network, a transportation network, a communication network, etc.

What is Internet fraud:
Internet fraud refers to the act of using the Internet to defraud a large amount of public or private property by fictitious facts or concealing the truth for the purpose of illegal possession.
There are many forms of fraud, and the methods of fraud are changing with each passing day. Common methods include impersonating friends, phishing, and online banking upgrade fraud. The main features include space virtualization and behavior concealment.

What is network security:
Cyber Security refers to the protection of the hardware, software and data in the network system, which will not be damaged, changed or leaked due to accidental or malicious reasons, and the system will run continuously, reliably and normally, and the network service will not be interrupted.

How to prevent fraud:
Do not provide important information such as ID number, home address, and work unit to strangers. Do not save your ID photo or ID number in your mobile phone to avoid personal information leakage.
When receiving strange calls or text messages, especially those claiming to be from a bank or public security officer, be vigilant and do not trust information from strange numbers.
Be suspicious of sudden winning news, do not click on links or provide personal information easily.
Choose regular platforms to shop, check the seller's information, and avoid buying goods on unfamiliar small platforms or through social software.
When looking for a job, do not pay fees easily. Regular companies will not ask applicants to pay deposits or training fees.

Ruthlene:
The pace at which the threat vectors in digital technology continue to change has been impressive. Cybercrime applies scams, hacking, and identity theft as a means of fraudulently acquiring sensitive information. These criminals make use of the unsuspecting individuals and businesses as their main target. From phishing emails and websites to financial fraud and major data breaches, the scams are more sophisticated now than ever before.

As cyber threats are on the rise, awareness and prevention are even more important. Strong passwords, two-factor authentication, and identification of scam messages can greatly minimize the risk of falling prey to scams.Also, the adoption of cybersecurity best practices will raise awareness of emerging threats, hence securing individuals' and organizations' assets in cyberspace.

Whether one will be in a position to gain full benefits from online opportunities or not depends on how an individual can avoid cyber scamming with prior knowledge about its

working and methods of prevention. This discussion, therefore, summarizes the impact caused by cyber scams, the level of cybersecurity awareness, and main steps toward becoming protected in today's digital context.

Isabel:
Cybersecurity is the practice of protecting and defending computer systems, networks, cloud infrastructures, and more from online threats. With the growth of the internet and digital services, including cloud computing, data storage, and digital applications, the number of cyber-attacks has risen significantly. This increase in digital engagement enables users to participate in a wider range of more profitable cyber crimes, including phishing, email spam, and account takeover fraud.

Effective cybersecurity requires the cooperation of people, technology, and processes to guard against cyber dangers. Users must comprehend the principles of cybersecurity, remain alert, and follow best practices such as utilizing strong passwords and exercising caution with email attachments.

Organizations must establish a strong framework to effectively address cyber threats, ensuring they can identify, protect, detect, respond to, and recover from incidents. Technology is vital in this defense strategy, offering tools such as firewalls, malware protection, and antivirus software to shield endpoints, networks, and cloud systems. Collectively, these components form a holistic approach to cybersecurity.

Jie Ying:
Cybersecurity protects computers, networks, and data from threats like hacking, viruses, and scams. It started with basic security measures like passwords and firewalls but evolved with advanced protections such as encryption, multi-factor authentication, and AI-based systems. Today, it is crucial for individuals and businesses to safeguard their information.

Many fall victim to online scams due to a lack of awareness and weak cybersecurity, leading to financial loss and identity theft. Better education and stronger security measures are needed to prevent these threats.

With the rise of scams, here are some key ways to stay protected. First, use strong passwords and avoid using personal details like IC or phone numbers. Enable multi-factor authentication for extra security. Second, avoid clicking on suspicious links and keep software updated to fix security flaws. Enable firewalls and antivirus software to block threats. Always verify sources before sharing personal information and stay informed about the latest scams. Use secure networks, avoid public Wi-Fi for sensitive transactions, and consider a VPN for extra protection. Regularly monitor bank statements and online accounts for suspicious activity. These steps help reduce the risk of cyberattacks and online fraud.

Nadhrah:
Scamming in the world of cybersecurity refers to when a scammer tricks you online by stealing your personal information or money. Their tactics include using fake emails,

websites, or send fake messages in order to get you to share personal information like passwords or credit card numbers. Other examples include malware attacks, where they would send bad software that infects the computer, ransomware attacks, which they lock your files and ask for money to be able to unlock it again.

Myra:

Cyber security is key to protecting personal and business data from potential threats in this digital world. Scams like phishing, spoofing, and scareware are becoming increasingly common, so users need to be stove-pipe, take precautionary measures and ensure that their data is protected. Phishing, for instance, uses misleading emails to entice users into disclosing sensitive data, whilst spoofing imitates genuine sources to steal credentials. To avoid this type of fraud, a proactive stance must be taken, such as authenticating the message, using strong and unique passwords, enabling two-factor authentication, etc. With knowledge and implementation of these practices, one can mitigate the risk of cyber threats to a great extent.

Problem Statement:

Rachel:
In recent years, online scams have become a major cybersecurity concern in Malaysia, it has leading to significant financial losses and compromised personal data. Based on the report from CyberSecurity Malaysia, the number of scam-related incidents keeps increasing which include phishing, fake investment schemes and online shopping fraud. Despite the efforts of authorities and cybersecurity organizations, many Malaysian still lack of necessary awareness to identify and prevent these scams.

Additionally, as online scam cases continue to increase, the effectiveness of existing cybersecurity education programs remains uncertain. Without a greater emnphasis on cybersecurity awareness and digital literacy, individuals and business will remain vulnerable to financial and data-related threats. Therefore, we aim to emphasize the role of cybersecurity awareness in scam prevention and increase the awareness of cybersecurity especially on the prevention of scams of the public.

Jia Wenbing:

With the popularization of the Internet, online fraud methods emerge in an endless stream and have become an important issue affecting social security. Criminals use false information, forged identities, impersonating customer service, investment and financial fraud, etc. to induce victims to be deceived. They often take advantage of people's trust or greed for cheapness to defraud victims of their money through carefully designed scams. Due to the anonymity of the network environment and the continuous upgrading of fraud methods, many users fall into scams without knowing it, causing serious economic losses and personal information leakage.

Online fraud not only affects personal property safety, but may also endanger the trust system of society, causing the public to panic about online transactions and information security. Therefore, raising the public's awareness of network security and popularizing anti-fraud knowledge have become the key to dealing with this problem.
This study will enhance the public's awareness of network security and how to better prevent network fraud. By strengthening personal prevention measures, at the same time, the government and relevant agencies should increase supervision and improve technical means to combat network fraud, and jointly create a safe and trustworthy network environment.

Liu Ziyu:
Why are there so many online scams in today's society? What causes them? How can we solve them? How can we prevent them?

Ruthlene:
Cyber fraud has now grown into a serious threat in this digital world and keeps on growing. Starting from phishing emails, to fake websites, identity theft, and financial fraud, cyber criminals somehow always find new ways through which they easily deceive the public and make them fall into scams. These scams not only bring financial loss but also emotional distress, personal privacy breaches, and sometimes even the ruin of lives. Yet, even with increased awareness, many individuals and businesses continue to get hit because of a lack of knowledge, weak security practices, or just being caught off guard.

The more personal and financial information are placed online, the higher the risk from cyber scams. Many people will grossly underestimate just how sophisticated these scams have become and believe themselves to be too smart for scammers-until it finally happens to them. Traditional measures of security cannot cut it anymore, nor can anybody hope to be one step ahead when proactive steps such as strong passwords, enabling two-factor authentication are absent, if one cannot notice the red flags.

The study is going to emphasize the gravity of cyber scams, reveal common vulnerabilities, and explore practical steps to prevent them. Understanding how these scams work and developing better cybersecurity habits can help individuals and organizations protect themselves and create a safer digital space.

Isabel:
With the rapid growth of the internet and digital applications, cybersecurity threats have also rised, including phishing, email spam and account takeover fraud. There is a lack of awareness and practices as many users fail to follow cyber security ptactices as well such as, using strong password and email verification attachments which makes them easy targets to attacks.

Organizations also often find it challenging to create an reliable cybersecurity framework, which leaves their systems, networks, and cloud environments exposed to numerous threats. Although technology provides crucial security components like firewalls and antivirus solutions, cybercriminals are constantly adapting their tactics, making traditional defenses insufficient. This growing complexity of cyber threats underscores the necessity for a comprehensive approach to cybersecurity. Achieving effective protection demands a collaborative effort from individuals, organizations, and technology to identify, safeguard, detect, respond to, and recover from cyber incidents. By incorporating robust security measures, ongoing monitoring, and user education, organizations can enhance the protection of their digital assets and lessen potential risks.

Jie Ying:
As technology advances, online scams are increasing, with many falling victim due to weak cybersecurity awareness and poor security practices. Hackers exploit vulnerabilities through phishing, weak passwords, and unverified links, leading to financial loss and identity theft. With AI advancements, scammers can now mimic voices and faces, making fraud even more convincing. Without proper education and preventive measures, individuals remain at high risk. Therefore, strengthening cybersecurity knowledge and implementing better security practices are crucial to reducing these threats.

Nadhrah:

Online scamming has become a significant threat in the digital world, where cybercriminals deceive individuals and organizations into revealing sensitive information or transferring money. These scams take various forms, including phishing emails, fraudulent websites, fake messages, malware attacks, and ransomware. Victims often unknowingly fall prey to these tactics, leading to financial losses, identity theft, or compromised data security.

The increasing sophistication of these cyber scams poses a major challenge for individuals and businesses, as attackers continuously adapt their strategies to bypass security measures. There is a need for better awareness, stronger cybersecurity defenses, and proactive measures to prevent these scams from causing harm.

Myra:

With the fast-paced plan of present day digital technology, the fear of cyber threats is to be found everywhere, putting individuals and organizations into critical losses. Malicious attacks like phishing, spoofing, scareware, etc. are more sophisticated than ever; detecting and avoiding these scams has become a complex task for common users. Although security tools are available, ignorance and insufficient prevention have left many susceptible to data breaches, financial loss, and compromised personal information. As cyber attacks become more common, there is an increasing need for effective strategies and teaching people about cyber security so that they can be prepared in future and can protect themselves in a digitized world.

Case Study:

Rachel:

Cybersecurity Incidents Report by Cyber999 (2024)

From January 2024 to October 2024, CyberSecurity Malaysia's Cyber Incident Response Centre (Cyber999) has recorded 5181 cybersecurity incidents. The majority of the incidents were online fraud cases which has a total 3483 cases, 67.23% of the recorded incidents, followed by content-related issues (480 cases) and malicious code incidents (403 cases). An average 500 cases have been recorded every month.

"All the cases we receive involve online users, and this threat has a significant impact on the country, with losses amounting to millions of ringgit," according to CyberSecurity Malaysia chief technology officer Wan Roshaimi Wan Abdullah.

https://thesun.my/malaysia-news/cyber999-records-5181-cybersecurity-incidents-from-january-to-october-this-year-HH13277990?utm_source=chatgpt.com

Impact of Online Scams in Malaysia (2021 - Apr 2024)

From 2021 to April 2024, Malaysia experienced a significant surge in online scams resulting in substantial financial losses and affecting a large number of individuals. Malaysia has lost a total of 3.18 billion Malaysian Ringgit due to online scams during this period, over 95800 individuals fell victim to various online scams. The significant financial losses and high number of victims could be higher due to many victims may not report scams due to embarrassment or lack of awareness.

Common types of scams are Phishing, Investment Scams, Online Purchase Scams.
Phishing: Fraudulent attempts to obtain sensitive information by disguising as trustworthy entities via electronic communications.
Investments Scams: Deceptive programs that promise high returns on investments that actually dont exist or worthless.
Online Purchase Scams: Fake e-commerce platforms or sellers that defraud consumers by selling non-existent product or failing to deliver goods after payment.

https://vir.com.vn/malaysia-loses-700-million-usd-due-to-online-scams-113572.html?utm_source=chatgpt.com

Jia Wenbing:

Swindlers swindled 54 billion yuan in one year (2025)
In Malaysia, the amount of money lost due to online fraud cases each year is as high as RM54 billion, accounting for 3% of the gross domestic product (GDP), which is surprising and worrying!

"Bernama" reported that online fraud cases are not only a threat to individuals, but also have a far-reaching impact on the global economy and have a long-term impact on the growth of the national economy. Therefore, small and medium-sized enterprises that are entering Malaysia for the first time need to be more vigilant against fraud cases.

The report said that after the scammers saw that they could easily "make money" from the scams they set up, they joined this illegal "industry" and eventually set up fraud bases in countries such as Myanmar and Cambodia. The scammers also kept up with the times and used advanced technology, including artificial intelligence (AI) to commit fraud.
https://www.chinapress.com.my/20250107/%e5%a4%a7%e9%a9%ac%e4%ba%ba%e5%be%88%e5%a5%bd%e9%aa%97-%e8%80%81%e5%8d%83%e4%b8%80%e5%b9%b4%e5%8d%b7%e8%b5%b0540%e4%ba%bf/

A salesperson in a telecommunications fraud case outside Malaysia was suspected of fraud, and the amount of fraud was 290,000 yuan. The accomplice did not return the money and was sentenced to two years (204)
The procuratorate accused Lu of setting up a criminal group that carried out telecommunications network fraud in Kuala Lumpur, Malaysia from June 2019 to February 2020.
The fraud group provided speech training, distributed mobile phones and WeChat numbers, formulated basic salary and commission rules, and set up positions such as director, agent, supervisor, team leader, and salesperson.
The salesperson was arranged to meet the victim through social software, deceive the victim's trust with a fictitious identity, and then send the victim a link to the "XXbao" APP to induce the victim to download, and defraud the victim's money by blocking withdrawals or controlling wins and losses in the background.
From June to October 2019, Zhang worked as a salesperson in the fraud group, responsible for meeting the victim through social software and diverting them to the APP involved in the case. During this period, the fraud group defrauded the victim of 290,000 yuan.
In May 2023, Zhang was arrested by the public security organs and confessed the crime truthfully after being arrested.

https://zhuanlan.zhihu.com/p/11950602196

Liu Ziyu:
Case 1:
A Malaysian man met two "beauties" through social media. The "beauties" told him that they were trapped in northern Myanmar. One of the "beauties" said that her cousin opened an

entertainment company in Thailand and urgently needed a translator. He was so overwhelmed by love that he went to Thailand alone. Somehow he was taken to the KK Industrial Park in Myanmar and forced to become a "piglet" for recruitment and translation. Later, it was discovered that the "beauties" were actually a man who played two roles and directed and acted in his own drama. After being trapped for seven months, he escaped with the help of Mr. Huang, a Malaysian Thai businessman, and was rescued by the police and returned to Malaysia.
Case 2:
A Chinese male cram school teacher applied for a job as a translator at a Thai bank through the Internet. Unexpectedly, after arriving in Bangkok, Thailand, he was kidnapped by the person who greeted him and taken to the KK Industrial Park in Myanmar. After arriving at the industrial park, he met another local man who said that he went to Thailand because he mistakenly believed that he would get a considerable reward after successfully borrowing his identity to get a loan. The fraud group threatened that it would only take a week to complete the loan procedures and let him return home. Now, a year later, they still can't escape the purgatory-like life and regret their decision to work abroad. Using stolen mobile phones to reveal the new methods used by the fraud group. In addition to online dating and high-paying jobs, they also use "loans in exchange for remuneration" as bait to lure victims.
https://zhuanlan.zhihu.com/p/19486078156?utm_id=0

Ruthlene:
LINK
Case Study: The Escalating Threat of Online Scams in Malaysia
Malaysia saw a drastic increase of online scams over the last two years during the Covid-19 pandemic. According to the Royal Malaysia Police's (PDRM) commercial crimes investigation department (CCID), a total of 71,833 scams, amounting to more than RM5.2 billion losses, was reported from 2020 until May 2022.

From the total amount of scams, 48,850 or 68% were online scams, where 26,213 cases were prosecuted in court. 5,851 e-commerce scam cases was recorded in 2020 followed by 9,569 cases last year. Up to May this year, 3,833 cases were recorded.

The other types of scams include job scams (350 cases) and loan and investment scams (11,875 cases).

Isabel:
Increase in harmful social media content
https://www.reuters.com/technology/malaysia-seeking-social-media-platforms-commitment-tackle-cybercrimes-2024-07-24/

Overview: In the first three months of 2024, the government referred **51,638 cases** to social media platforms for further action, up from **42,904 cases** recorded in the whole of last year,

according to the Malaysian authorities. Fahmi said Meta had the highest compliance rate with the government's request to remove harmful content found on its platforms, with Facebook recording a compliance rate of 85%, Instagram at 88% and WhatsApp with 79%.

Malaysian authorities deem online gambling, scams, child pornography and grooming, cyberbullying and content related to race, religion and royalty as harmful. Meta and TikTok restricted a record number of social media posts and accounts in Malaysia in the first six months of 2023, data published by the firms last year showed.

Jie Ying:

Unsolicited Package Scam

- Scammers send random parcels to recipients and demand payment upon delivery.
- A woman in Perak received a mysterious package with an RM198 payment request but refused it.
- Source: The Rakyat Post

Calling Scams

In Malaysia, phone scams have led to significant financial losses. Between 2021 and 2023, authorities recorded 8,011 phone scam cases, resulting in losses totaling RM440.9 million.

thestar.com.my

In one notable incident, a retired banker from Ipoh lost approximately RM1.44 million after being deceived by individuals posing as officials from the Malaysian Communications and Multimedia Commission (MCMC) and the police.

bernama.com

Nadhrah:

Risk of MyKad Data Leakages (2024)

Background:
In December 2024 many data leakage concerns in Malaysia were brought up including this issue of Malaysia's national Identification system, MyKad. Allegedly the identity information of 17 million Malaysians was leaked, which raised the concern of identity theft and financial fraud.

Details of the breach:
A Singapore-based dark web intelligence agency called Stealth Mole shed light about the issue, reporting that malicious actors were selling MyKad data on the dark web. Multiple

MyKad cards were shared as proof of the breach. Information like full names, id numbers, addresses, and biometric information was leaked which poses a major risk.

Response:
The National Cyber Security Agency (NACSA) initiated an investigation to find out the authenticity of the breach and how major it is. They emphasized the seriousness of the case and assured the public their dedication to getting to the bottom of it.

https://fintechnews.my/47086/cyber-security/mykad-data-leak-raises-concerns-over-financial-fraud/#:~:text=A%20major%20data%20leak%20has,identity%20theft%20and%20financial%20fraud.

Myra:

The Macau Scam in Malaysia involves fraudsters posing as officials from agencies like the police or Bank Negara, tricking victims into transferring money to resolve fake criminal charges such as money laundering or theft. Common tactics include impersonation, false credit card claims, and fake lottery winnings. Victims are often seniors, wealthy individuals, or easily distressed people. The scam has caused significant financial losses nationwide. Awareness and immediate reporting are crucial to prevent falling victim.

https://siberkasa.cybersecurity.my/articles/macau-scam