Response to Text (20%)

Based on the output of your group discussion, transfer the information into the table below. You may extract the main ideas from the source text into the first column of the table. From the main idea, you need to summarise or paraphrase the source text extracted. You will also need to combine your point with another main idea from your group member. You may refer to this table to write your report.
This reading table must be submitted to your instructor. This assessment will be marked individually.

Title: Cybersecurity Threats Increases Rapidly

Problem statement: Cybersecurity Threats Are Harmful Towards Human

COLUMN 1 **Source text**	**COLUMN 2** **Main ideas from the text (extracted from source text)**	**COLUMN 3** **Summarise/Paraphrase**	**COLUMN 4** **Synthesis (combine your own point and another group member's point)**
NAME (MATRIC NO): CHUA JIA LIN (A23CS0069) **Text 1** Title: Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours	The results demonstrated that Internet addiction was a significant predictor for risky cybersecurity behaviours. A positive attitude towards cybersecurity in business was negatively related to risky cybersecurity behaviours. Finally, the measure of impulsivity revealed that both attentional and motor impulsivity were both significant positive predictors of risky cybersecurity behaviours, with	According to Hadlington (2017), individuals who spend excessive time online or act impulsively tend to make poor decisions regarding online safety. On the other hand, people with a positive attitude towards cybersecurity are more cautious and responsible in their online behaviour. According to the study, planning ahead helps to reduce risky behaviour, while being easily distracted or impulsive increases it.	Both Hadlington (2017) and Bada et al. (2019) emphasise that staying safe online is not just about knowing cybersecurity tips; it also depends on whether people actually apply those tips in their daily lives. According to Bada and his team, most awareness campaigns are ineffective because they fail to change people's behaviour. Similarly, Hadlington noticed that people who act impulsively or spend excessive time online are more likely to make risky

Source reference: Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346	non-planning being a significant negative predictor.		decisions, such as clicking suspicious links or ignoring security advice. Combining both studies shows that effective cybersecurity requires more than information; it also involves developing good habits and behaviour.
NAME (MATRIC NO): LAU YEE WEN (A23CS0099) **Text 2**	"Phishing attacks, which have existed for several decades and continue to be a major problem today, constitute a severe threat in the cyber world."	Alabdan (2020) points out that phishing is made up of three mutually supportive elements the medium (e.g., email, SMS), the vector (how it is delivered), and the technical approach (e.g., malware,	As demonstrated by Alabdan (2020), phishing is an organised and threatening attack that consists of several technical layers. I concur that spear phishing is particularly malicious as it specifically attacks

Title: Phishing Attacks Survey: Types, Vectors, and Technical Approaches Source reference: Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168	The phishing techniques discussed in this paper are split into three key groups that are interconnected. These are: The medium, The vector, The technical approach." "Spear phishing is the most common infection vector for the distribution of malware, used by 71% of groups in 2018 and 65% of groups in 2019." "Furthermore, the number of phishing Uniform Resource Locators (URLs) increased by 20% between 2017 and 2018. " "Phishing also played a part in the first successful cyber attack on a power grid, which took place in Ukraine in December of 2015. IT staff and network administrators of various companies that handled power distribution for Ukraine were targeted with spear phishing attacks."	XSS). This structured and evolving nature makes phishing increasingly sophisticated. Among these, spear phishing remains the most dangerous, often serving as a delivery method for advanced malware and targeted attacks. Real-life implications may be catastrophic—Alabdan offers an example of 2015 cyberattack on the Ukraine's power grid when a phishing campaign successfully dropped power to more than 230,000 users and showed that phishing can be used not to target individuals, but destroy infrastructure as well.	the victims and has a tendency to deliver dangerous malware. Along with the argument of my group member that phishing can not only harm a person, but also entire systems such as power grids, it is evident that phishing is not just a personal threat, but a threat to national security and public infrastructure. This explains why phishing detection and prevention measures need to be improved urgently.

NAME (MATRIC NO): CHERYL CHEONG KAH VOON (A23CS0060) **Text 3** Title: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Source reference: Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672	Unfortunately, many individuals do not comply with specified policies or expected behaviours. There are many potential reasons for this, but two of the most compelling are that people are not aware of (or do not perceive) the risks or they do not know (or fully understand) the 'correct' behaviour.	In addition, user behaviour is also a contributing factor. A common issue is that many users do not understand the risks they face or the effects of their behaviours(Bada, Sasse &Nurse, 2019). This lack of awareness can result in risky online behaviour, such as clicking suspicious links or sharing sensitive data online, which reduces the overall cybersecurity system	This point aligns with Hadlington (2017), who found that people with high impulsivity are more likely to take online risks. Both studies suggest that simply having rules or laws is not enough—users must also be aware of risks and understand safe behaviour. Therefore, besides legal reform, user education and awareness campaigns are essential to reduce cybersecurity threats.

NAME (MATRIC NO): GUI KAH SIN (A23CS0080) **Text 4** Title: Pig Butchering in Cybersecurity: A Modern Social Engineering Threat Source reference: Burton, S. L., & Moore, P. D. (2024). *Pig butchering in Cybersecurity: a modern social engineering threat*. Scholarly Commons. https://commons.erau.edu/publication/2266/	The emotional manipulation involved in pig butchering scams results in significant psychological trauma (Montañez et al., 2020). Victims often experience intense feelings of stress, anxiety, and depression. These psychological effects are exacerbated by the realization that their trust has been exploited, which can lead to feelings of humiliation and guilt (Whittaker et al., 2024). The financial losses further compound these emotional wounds, creating a cycle of stress and anxiety that can be difficult to break. Research has shown that victims of such scams often suffer from long-term psychological effects, including chronic stress and the potential development of mental health disorders like post-traumatic stress disorder, PTSD (Curtis & Oxburgh, 2022). The betrayal of trust and significant financial loss can alter a victim's perception of safety and trust in others, leading to long-term psychological distress	According to Burton and Moore (2024), pig butchering scams cause not only financial harm but also severe emotional and psychological distress. Victims often experience overwhelming stress, anxiety, and depression, especially when they realise their trust has been manipulated. The sense of betrayal will then further intensify their emotional suffering. In many cases, the psychological impact is long-lasting, potentially resulting in chronic stress or mental health infections such as post-traumatic stress disorder (PTSD). Besides, these scams will also damage their ability to trust others.	Burton and Moose (2024) emphasise the serious emotional and psychological effects faced by the victims of pig butchering scams, including anxiety, depression and PTSD. Likewise, Alabdon (2020) illustrates the impact of the other insights, which focus on how phishing has become a sophisticated cyber threat capable of targeting critical infrastructure, as seen in the Ukraine power grid attack. Therefore, both perspectives show that cybercrimes today are not only technically advanced but also cause deep personal and societal harm; the need for comprehensive responses like cybersecurity measures and psychological support for victims is vital.

	(Curtis & Oxburgh, 2022; Wang, 2024).		

List of references

Hadlington, L. (2017).
Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672

Burton, S. L., & Moore, P. D. (2024). *Pig butchering in Cybersecurity: a modern social engineering threat*. Scholarly Commons. https://commons.erau.edu/publication/2266/