***What does it do? (600 words)***

**What is the state of the art of this technology?**   
As of now, cyber security is the go-to for safety measures when browsing the internet, but one thing to keep in mind while browsing the internet is that its rather easy to fall victim to cases such as Credential stuffing, Spear phishing and Ransomwares if you are not careful. All of these cases involve stealing or hacking into an account and taking sensitive information for their own benefit. (Whitehead, 2020)

Ever since the covid-19 outbreak in 2020, the number of data breaches increased significantly due to malicious hacking. With the number of people working from home increasing it is no surprise that the types of incidents that happened changed and not for the better. Data breaches were doubling, and ransomwares were on the decline compared to previous years. Because of this, citizens and industries had to be flexible in terms of online safety, otherwise they risk getting their sensitive information taken by hackers.  (Akamai, 2021)

**What can be done now?**

In order to be better protected, it is important to know what types of cyber security there are. Some examples would be critical infrastructure security, network security, application security, information security, cloud security, data loss prevention, and end-user education. An explanation on what each of these terms do is listed below. (Akamai, 2021)

* **Critical infrastructure security**: Consists of cyber-physical systems such as electricity grid and water purification systems. (Johansen, 2020)
* **Network security**: Protects internal networks from intruders by securing infrastructure. Examples of network security include the implementation of two-factor authentication and new, strong passwords. (Johansen, 2020)
* **Application security**: Uses software and hardware to defend against external threats that may present themselves in an application’s development stage. Examples of application security include antivirus programs, firewalls, and encryption. (Johansen, 2020)
* **Information security**: Also known as InfoSec, protects both physical and digital data—essentially data in any form—from unauthorized access, use, change, disclosure, deletion, or other forms of malintent. (Johansen, 2020)
* **Cloud security**: A software-based tool that protects and monitors your data in the cloud, to help eliminate the risks associated with on-premises attacks. (Johansen, 2020)
* **Data loss prevention**: Consists of developing policies and processes for handling and preventing the loss of data and developing recovery policies in the event of a cyber security breach. This includes setting network permissions and policies for data storage. (Johansen, 2020)
* **End-user education**: Acknowledges that cyber security systems are only as strong as their potentially weakest links: the people that are using them. End-user education involves teaching users to follow best practices like not clicking on unknown links or downloading suspicious attachments in emails—which could let in malware and other forms of malicious software. (Johansen, 2020)

A good example of cyber security done well is Nord VPN. Not only does it provide the services stated above, but it also provides you with a secure, encrypted tunnel for online traffic flow. You are the only one that can see through this tunnel, nobody else can so its great if you are looking for peace of mind when browsing the internet. Additionally, it secures personal information or work files, encrypts your internet connection so you can connect to public Wi-Fi without any difficulties, while keeping your browsing history private.  (NordVPN, 2021)

**What is likely to be done soon?**   
While researching future investments for cyber security, I found out that machine learning is making progress within the online industry but will need an ongoing investment. From my perspective, I see a lot of potential, it just needs better automation and predictive reasoning, so artificial intelligence (AI) still has room for promise. (Whitehead, 2020). I expect that 25 years from now that it will become a lot more commercialized, so it will be expected that the AI will be able to predict behavior patterns if it needs to. Therefore, if a large company such as Tesla was to invest into AI, the impact it would have on the economic side would be dramatic. This is due to the fact that AI can dramatically improve efficiency of workplaces, in addition to contributing indirectly to other areas, like cybersecurity. (Whitehead, 2020)

**What technological/other developments that make this possible**

As of now, we have seen a lot of improvement in terms of security being incorporated into normal product offerings. Especially in the last 5 years, the integration and offering of security as part of a normal package has really changed the landscape. This is due to cloud providers, such as Microsoft and Google, incorporating a lot of security at a remarkably high level that was traditionally only available through third-party solutions. Thus, many things will be able to be automated because of innovation. (Whitehead, 2020)

As a result, it has become more challenging for organizations, consumers, and even CISOs to keep track of the different spots where security is provided and to have it all come together from the same perspective. So in the near future, I think we are going to see trends towards consolidation, as well as trying to make the information obtainable into consumable amounts that don’t force you to dig as deep into the abyss to understand your risk. (Whitehead, 2020)

***What is the likely impact? (300 words)***

**What is the potential impact of this development and what is likely to change?**    
The potential impact of these developments could lead to a higher standard for cyber security. This will lead to more demand for security intelligence, so the need for suitable candidates will grow. For this reason, workers that have these required skillsets will receive a higher salary as the years go on.

**Which people will be most affected and how?**

Cyber security will be able to help everyone since it allows users to browse the internet without having to worry about any malicious intention’s attackers may have. It can successfully change IP addresses and hide ISP information (Internet service Provider). Not only that, but it encrypts any sort of transaction to make sure it isn’t tracked by anyone, only you can see it.

**Will this create, replace, or make redundant any current jobs or technologies?**   
Since there is a limit to how much technology can do by itself, it is important to know that sophisticated cyber attackers will break through the barriers eventually if they are not looked after. Therefore, a need for security intelligence is required. Technology has its weaknesses, and attackers aren’t afraid to take advantage of them, so it is important to identify and address them efficiently. Since the safety requirements are only increasing as time goes on because of the increased digital use, more anomalies are occurring, thus creating more job opportunities for cyber intelligence.

***How will this affect you? (300 words)***

**How will this affect me in my daily life?**   
Personally, this will not affect me that much since I work in customer service. However, the more we invest in cyber security, there will be a greater need for cyber intelligence to keep these types of technologies operational and optimized. As time goes on, the demand for cyber security will increase, which will lead to a higher salary and the need of a certain skill set (Data, 2019). In this way it would be impactful to people since it would encourage people to spend more time studying than spending time with family.

**What will be different for you?**   
The main difference for me will be the upkeep of knowledge. The knowledge to understand advancements taken in both ends to properly defend myself from attackers, but with the services such as Nord VPN, protecting myself for any malicious intentions that will be significantly easier.

**How might this affect members of your family and friends?**   
Growth in this industry will lead to many positive aspects on my family personally. This can also provide a layer of protection when looking around the internet or doing any sort of transaction, be it over the internet or crypto. So, in my opinion, having more job opportunities open up in the near future will be beneficial, but could easily be the main cause of stress for several families.

# **Bibliography**

Akamai. (2021, July 10). *Satae of the Internet.* Retrieved from Akamai: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-gaming-in-a-pandemic.pdf

Australia, B. (2021, March 15). *How COVID-19 has shaped the cyber security landscape*. Retrieved from BDO Australia: https://www.bdo.com.au/en-au/insights/cyber-security/articles/how-covid-19-has-shaped-the-cyber-security-landscape

Data, I. o. (2019, October 28). *Is cyber security in demand in Australia?* Retrieved from Institite of Data: https://www.institutedata.com/blog/is-cyber-security-in-demand-in-australia/

Johansen, A. G. (2020, July 24). *What is cyber security? What you need to know*. Retrieved from Norton: https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html

NordVPN. (2021, July 8). *What are the risks of not using VPN*. Retrieved from NordVPN: https://nordvpn.com/country/australia/?vpn=brand&gclid=CjwKCAjwuIWHBhBDEiwACXQYsa4XZERlCokD8LLleiH4U1v5gzoc5z8Th3KOTC44knb457wuyHRJXRoCVzcQAvD\_BwE

Whitehead, M. (2020, November). *What is the Future of Cybersecurity?* Retrieved from Trustware: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-is-the-future-of-cybersecurity/