CyberSecurity

Cybersecurity is a technology which protects internet connected systems from harm over the internet. The purpose of cybersecurity is to protect data or the users system from any potential threats over the web. These threats could be programs such as Malware, Ransomware or even Phishing. Malware is a type of software which can cause files or programs used to damage the computer. Some examples of this are viruses and spyware. How a virus works is that it attaches itself to a pure file and then infects other files. It spreads rapidly and can damage or even destroy files or a system. On the other hand, spyware is made to spy on the user. It tracks what the user does online and the things they input, such as passwords or even credit card details. Cybersecurity is an always changing and growing area since the development of technology could also lead to new types of threats to the computer like ransomware; which is a type of malware which locks the users files and demands a “ransom” to unlock the file. This is typically a payment. Phishing is a type of fraud where fake emails are sent to users which look professional and resemble big organisations in order to take important information from the user.

As the different types of malwares increase, there are also security measures to prevent users from falling victim to these threats. Many countries and businesses have invested billions of money into Cybersecurity to protect confidential information which are important to the business. Gartner, a big IT company also predicted that this value will only increase as the years go by. Traditionally, companies and governments have focused their main resources on the most crucial and important information data files which is a smart idea, but it also leaves other pieces of information left protected with minimal effort which leads it to often be leaked or damaged. It is important for businesses to implement cybersecurity measures to PREVENT the damage to files rather than find a solution to fix the damage afterwards. There are numerous types of cyber security. These are some of them;

- Network Security

  The basis of this is to protect the internal networks from those who are trying to access the computer from the outside by securing the core of the CPU. Network Security is primarily focused with the networking area of the business. This deals with problems with routers and switches which are known as data transport mechanisms. The main difference between network security and information security is the process of planning.
- Application Security

  This uses both soft and hardwares to defend the computer against any external threats which could be in attendance during the building stage. This could be antivirus programs or firewalls. Since the user would be using multiple applications to complete tasks, they could access these applications over networks which could be open or filled with threats. Security for these applications can minimize the chance of manipulation of applications to infiltrate and either access,steal, or even delete important information. One of the most common forms of application securities is a firewall which limits the accessibility to a file with the usage of specific programs.
- Information Security

  This protects the physical and digital data a user has on their computer from any unauthorised access. To prevent these attacks and minimise weaknesses within a system, there are many security controls which are implemented as part of a multi layered levels of defence. With numerous prevention measures put in place, the attack should be kept minimum. For additional defence businesses should put in place an incident response plan to limit damage once there is a security breach.

There are a number of trends which are currently happening and will continue to change within the next few years. Some of these are the increased usage of mobile phones or devices as a way to attack the user. Since usually each individual will carry with them a mobile device of some sort, making it an ideal way to target the user. Some expected occurrences in the next few years include the spending on cyber security. This will continuously increase as there is always a growing impact of malware on cyber security Artificial intelligence and machine learning are constantly growing, this could be a new target for those trying to threaten businesses information and details. Artificial intelligence will be a more important and impactful factor in both cyber attacks and defenses.

The effect of Cyber threats causes business owners and government officials to seek better and more effective methods of cyber security to counter these problems. Since these owners are worried of theft in important valuable information like personal records of customers or employees, they are likely to invest heavily in new cyber securities to further increase the defence on their data. This would create more jobs than currently because it is an ever growing field, there will always be businesses whether big or small who would want to have a team dedicated to protecting and securing their confidential documents. There is doubt that it would make some jobs redundant as there is an increased demand for securities to be put in place instead of taking this job away. This development will also impact me in my daily life. Since most individuals including myself use a computer/laptop and also carry a mobile phone around with me everyday. I would need to increase protection on these devices to ensure that my private information will not be accessed to by strangers or unknown parties. I am currently using a firewall as protection for my computer but I may need to upgrade to a well known antivirus security system such as McAfee or Norton in order to secure my information. There will be no significant difference for me as I am already aware of all the bad things which could affect me or my information and have already taken precautions for them. I may just need to upgrade these precautions if anything. This might affect members of my family as they also carry electronic devices on their personnel and use them everyday. I would need to recommend them to utilise these security measures as well to prevent them from receiving any cyber threats. Since prevention is better than a cure for these malwares and cyber threats.

References

https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/
https://searchsecurity.techtarget.com/definition/cybersecurity
https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html

https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/#2162e14b7ecc

https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/