Cyber Security: Causes Of Cyber Attacks And Ways To Prevent Them

In this modern era, almost everyone in the world uses the internet as this is beneficial to all of us because it makes our lives much easier such as we can use the internet to communicate like Facebook, Skype or Whatapps, we can access to bank, shop and more. As the usage of internet is increasing, the information from us are vital and it must be protected. I have decided to choose Cyber Security as the topic and I will be considering on how Computer Science will look in the future from Cyber Security. I will justify the reasons why I chose Cyber Security as the topic in Computer Science.

What is Cyber Security?

The main purpose of Cyber Security is used to keep the data protected from cyberattack such as hacker, malware, Disturbed Denial of Service (DDoS) and other more cyberattacks. It is not only just protecting the data, Cyber Security also protects computer system including hardware and software, software application and network.

Cyber Security involves safeguarding our personal information such as, bank accounts, medical information and other more important data. Cyber Security helps to decrease the danger of cyberattacks such as stop the hacker accessing to or damaging our important information.

What causes Cyberattack to happen?

When we use the computer, laptop or smartphones to access the internet, every time we seen multiple of websites and applications contains malicious that can infect on which devices you are using. Cyberattacks can be affected by human error or unintentional accident. However, those errors might be not accident and potentially intentional which gives an advantage to the hackers or cyberattack users to attack or steal confidential vital information. They have different type of tools that can damage our devices such as computer or laptop as they use viruses or malicious to give an opportunity to the unauthorised user to access the device. This can happen to us when we opened a strange email with an attachment which contains virus or selecting malicious website links or accidently install an unsafe software application which can cause the device to become infected and the data will be lost or stolen. This happens on almost last two years ago when the company called FACC sacked Walter Stephan, CEO of the Boeing and Airbus supplier after ‘fake president’ scam as the CEO thought the email was send from the president but it was the criminals who created phishing email which asked Walter to send money to the ‘fake president’. This affects the company as they lost $50million (roughly around £39million). The reason why they sacked the CEO because Walter Stephan breach the company’s rules as the company cannot afford to lose their important data and money otherwise they could be in serious trouble.

The users can make simple mistakes in obtaining precious data or poor social networking can lead the users to be in a hazardous situations as if the users do not make the account properly obtained then this will make it simpler for the hackers or cyberattack users to access the

account to steal data or money.

How to prevent cyberattacks?

To reduce the risk of cyberattacks, you must be more cautious and be prepared for cyberattacks. This will allow you to make sure that your organisation have the plan and strategies to stop the criminals such as back up all the important data and information. You must make sure that you install, update and use antivirus and antispyware software regularly on every computer which will reduce the chance of having viruses or malicious infecting the devices.

Make sure you use a Firewall for your internet connection as the Firewall is used to help a computer network from intruders such as hackers. Firewall does this by controlling what data can and cannot access it through it however, it is used to stop the malicious or viruses, unauthorised web user or prohibited software from giving an opportunity to the criminal accessing to the private network which connected to the internet. Firewall can be open with Windows and it is free to use. Make sure that your WIFI networks are safeguarded even if you have it in the workplace then ensure it is secured and hidden.

In the workplace, you must train the employees to make them learn, understand and be aware of the cyberattacks in Cyber Security principles. You should keep an eye on employees because they are in the business and they can able to access to the data. They could make simple mistakes like Walter opened a scam email. Make sure you limit the employees access to the unauthorised website or data, this will reduce the risk of cyberattack. You should check on how they use the passwords and keep the passwords safe from intruders. You can manage or create the password in your company. The password must be changed regularly to discourage intruders, for example, change the password after 90 days or less.

Carry out the Cyber Security risk assessment daily which this will lessen the risks. This will be beneficial to the company as it will keep them safe and prevent from losing their important information or data to competitors who are willing to steal some ideas.