**What is Cybersecurity? What makes it so important?**

Cybersecurity is a range of technologies, processes, and practices which protect data, devices, networks, and applications from anything sinister, ranging from unauthorised access to purposefully being damaged from a cyberattack. According to DNSstuff[20], the most common types of cyberattacks include: **SQL** **Injections**, which utilises malicious SQL code to access confidential information such as sensitive company or customer data[1]; **Phishing Attacks**, which is when the attacker poses as a trusted individual or company and tricks the victim through email, or text, into opening a malicious link, which will most likely lead to a malware being installed on the victims system[2]; and **Malware,** that refers to malicious software that can damage or freeze devices, steal sensitive data, and cause general chaos.[3]

It doesn’t matter who you are or how safe you are, no one is invulnerable from a cyberattack. In todays day and age, cybersecurity is one of, if not the most, necessary types of defence. In our modern society, access to technology is essential. Almost everybody uses some kind of computer and phone. On most of these devices, people keep all their personal information, like stored passwords, bank accounts, social media accounts, and private photos. Anyone can learn how to access and steal this information, with enough time and patience. Scamming someone and stealing their data, is as easy as sending an email, or borrowing their phone to “make a call”.

There are various ways to be protected, the main, of course, is downloading an antivirus/antimalware program, which can help to protect devices from malicious programs and individuals. This may seem like enough protection for some people. However, others use VPNs (Virtual Private Network) to route their internet connection through a providers private server, creating a “tunnel” which encrypts your data.

Over the many years that we have had computers, our safety has had to evolve with it. Back in the old days, before internet banking, social media, online gaming, etc., people did not have much to worry about. However, there were still malicious programs and people out on the World Wide Web, but there was less of a worry of people getting their information stolen from the internet. The first known computer virus was a worm named *Creeper* which would display a message saying “I’m the creeper: catch me If you can!” created by Bob Thomas in 1971. It was put onto ARPANET (a network which was the foundation of the internet we know today[6]) to spread to different computers and self-duplicate, as Creeper duplicated itself, it would erase older versions of itself[5]. In retaliation to this, Thomas’s friend wrote another program to delete any instance of Creeper appropriately named: *Reaper*. Thus making Reaper the first antivirus software.

Later, in 1989, the “Morris Worm” started to spread, which was the first DoS (denial of service) attack to spread around the internet, which affected around 6,000 computers. According to the creator of the Morris Worm; Robert Morris. It was designed to determine just how big the internet was, although what the worm would do was infect the same computer over and over thus slowing it down to the point of crashing. To rid the world of the Morris Worm, regional networks had to be disconnected for several days, shutting down the entire internet. From this, teams were created to tackle these kinds of issues; these teams were called Computer Emergency Response Teams, or CERTs for short.[4]

Then came the 90s, all new exciting technology! Easily accessible by the public, Tamagotchi’s for the kids! Phones which were inside of cars! Super HD realistic amazing graphics in video games! And the most exciting, VIRUSES! Anyone could upload anything, so why not upload viruses? They started primarily as pranks pulled by internet trolls, but later expanded into more complex infections, like trojans, spyware and malware. Unfortunately, CERTs couldn’t do a lot, yes they would fight the viruses, but they were just a response team. They could react and deal with the emergency when it came to be but could not prevent the outbreak from occurring. Because of this, antivirus software entered the field, which would fight the viruses, and save peoples data.[4]

Coming to now, we have cyber-attacks have drastically evolved. Cybercriminals are coming up with more malicious, creative, and challenging ways to obtain peoples data and ruin people’s lives. This comes to the question, what is the new state of the art technology regarding cybersecurity? Antimalware companies such as Symantec are using Artificial Intelligence and Machine Learning to “… analyse all of the data running into or out of an organisation to determine where the vulnerabilities of those systems lie.” [7] AI and Machine Learning can analyse data collected from millions of different incidents and utilise this knowledge to identify potential threats. Network-monitoring tools can also be used (which utilise AI) to gather the daily behaviour of users, and analyse the information collected to smoke out anything malicious, whether it be a program downloaded on the computer or a link someone clicked on in an email. Thus, making it harder for hostile threats to harm devices.[7]

However, this does not mean people cannot steal your information or data; it just makes it harder for harmful programs to access your data. Unfortunately, people can still steal your details from social media sites such as Facebook, or Instagram, and they can take information from your mailbox or mail which was thrown in the rubbish. They can download photos, take your name, and pretty much steal your identity. With the correct safety measures, this can be prevented, by privatising your profiles, limiting the amount of information uploaded onto these sites, putting a lock on your mailbox, and disposing of mail thoroughly.

According to Microsofts *CYBERSPACE 2025: Today’s Decisions, Tomorrow’s Terrain* there are three future scenarios as to what is going to happen. The first being **Plateau** which predicts that some countries can advance economically and socioeconomically with the use of technology, while others are left behind, causing a very uneven terrain for cybersecurity. The second **Peak,** which is when governments collaborate to promote strong open trades. In this scenario, businesses, governments and other organisations encourage the widespread use of technology, resulting in the accelerated growth of improved cybersecurity. The third scenario is **Canyon**, which has a limited use of ICT, causing none-to-slow growth of cybersecurity, due to the isolation, and obstructionist government policies, restricting trade amongst others and lessening economic and socioeconomic relationships with other countries. [8]

The most likely scenario out of these three is **Plateau.** Primarily because, some countries have been struggling to advance technologically, and this will continue for at least another decade. However, the world will be trying to push towards the **Peak** scenario; I do not think that the **Peak** outcome will occur for a while.

This would create more jobs in the cybersecurity sector, and in IT in general. With the significant demand for cybersecurity professionals at the moment, it means that if by 2025, the **Plateau** scenario or the **Peak** scenario occurs, there will be a more significant demand for cybersecurity professionals.

**How will this affect you?**

Every day I use my computer, smartphone, smartwatch, car head-unit, and online banking. All of my information like my name, phone number, address, etc., is accessible on all of these, with the correct safety measures such as; restricting what I upload, keeping my data as private as I can, and using antimalware programs, I have been keeping myself self and my family safe.

References

[1] Learning Center. 2020. *What Is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva*. [online] Available at: <https://www.imperva.com/learn/application-security/sql-injection-sqli/> [Accessed 20 October 2020].

[2] Learning Center. 2020. *What Is Phishing | Attack Techniques & Scam Examples | Imperva*. [online] Available at: <https://www.imperva.com/learn/application-security/phishing-attack-scam/> [Accessed 20 October 2020].

[3] What Is Malware? How Malware Works & How to Remove It. 2020. *What Is Malware? How Malware Works & How To Remove It*. [online] Available at: <https://www.avg.com/en/signal/what-is-malware> [Accessed 20 October 2020].

[4] Fruhlinger, J., 2020. *Top Cybersecurity Facts, Figures And Statistics For 2020*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html> [Accessed 20 October 2020].

[5] Techopedia.com. 2020. *What Is Creeper Virus? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/24180/creeper-virus> [Accessed 20 October 2020].

[6] SearchNetworking. 2020. *What Is ARPANET? - Definition From Whatis.Com*. [online] Available at: <https://searchnetworking.techtarget.com/definition/ARPANET> [Accessed 20 October 2020].

[7] Us.norton.com. 2020. *What Is Antivirus Software? Antivirus Definition | Norton*. [online] Available at: <https://us.norton.com/internetsecurity-malware-what-is-antivirus.html> [Accessed 20 October 2020].

[8] Query.prod.cms.rt.microsoft.com. 2020. [online] Available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtS> [Accessed 20 October 2020].

[9] Services, P., 2020. *Cyber Attack - What Are Common Cyberthreats?*. [online] Cisco. Available at: <https://www.cisco.com/c/en\_au/products/security/common-cyberattacks.html> [Accessed 20 October 2020].

[10] Digital Guardian. 2020. *What Is Cyber Security? Definition, Best Practices & More*. [online] Available at: <https://digitalguardian.com/blog/what-cyber-security> [Accessed 20 October 2020].

[11] Services, P., 2020. *What Is Cybersecurity?*. [online] Cisco. Available at: <https://www.cisco.com/c/en\_au/products/security/what-is-cybersecurity.html> [Accessed 20 October 2020].

[12] Software Reviews, Opinions, and Tips - DNSstuff. 2020. *Top 6 Common Types Of Cyberattacks In 2020 - Dnsstuff*. [online] Available at: <https://www.dnsstuff.com/common-types-of-cyber-attacks> [Accessed 20 October 2020].

[13] Nest. 2020. *The Fascinating Evolution Of Cybersecurity*. [online] Available at: <https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/> [Accessed 20 October 2020].

[14] AJ Willingham, C., 2020. *9 Tech Crazes That Made Us Lose Our Minds In The '90S*. [online] CNN. Available at: <https://edition.cnn.com/2017/08/10/us/90s-technology-fads-trnd/index.html> [Accessed 20 October 2020].

[15] En.wikipedia.org. 2020. *Reaper (Program)*. [online] Available at: <https://en.wikipedia.org/wiki/Reaper\_(program)> [Accessed 20 October 2020].

[16] Nortonlifelock.com. 2020. *Securing Against Malware Using Artificial Intelligence*. [online] Available at: <https://www.nortonlifelock.com/blogs/feature-stories/securing-against-malware-using-artificial-intelligence> [Accessed 20 October 2020].

[17] Nest. 2020. *Cybersecurity: One Million Job Openings And Counting…*. [online] Available at: <https://www.latrobe.edu.au/nest/cybersecurity-one-million-job-openings-and-counting/> [Accessed 20 October 2020].

[18] En.wikipedia.org. 2020. *Social Hacking*. [online] Available at: <https://en.wikipedia.org/wiki/Social\_hacking> [Accessed 20 October 2020].

[19]Palmer, D., 2020. *AI Is Changing Everything About Cybersecurity, For Better And For Worse. Here's What You Need To Know | Zdnet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/> [Accessed 20 October 2020].

[20] Software Reviews, Opinions, and Tips - DNSstuff. 2020. *Top 6 Common Types Of Cyberattacks In 2020 - Dnsstuff*. [online] Available at: <https://www.dnsstuff.com/common-types-of-cyber-attacks> [Accessed 20 October 2020].