**What does it do?**

Cybersecurity is the method of protecting systems, networks, and programs from digital attacks. These digital attacks are known as ‘cyberattacks’ and are usually carried out in an attempt to access/alter user information, wipe out information and extort users of their money. The different types of cybersecurity threats include phishing, ransomware, malware, and social engineering. To prevent such attacks there are a range of practices you can do like encrypting important information, backing up your data, installing security software, using multi-factor authentication and much more. As of lately, machine learning and AI are now becoming an essential technology for information security due to its ability to predict potential threats and help prevent similar attacks in the future. Within a few years machine learning will become a staple in cybersecurity as it provides automation in three areas of cybersecurity measures and that being:

* Threat Detection: AI analyzing data and recognizing patterns that may potentially lead to an attack
* Threat Response: AI can automatically carry out security protection procedures
* Human Augmentation: AI can alleviate the stress on IT security teams who are overwhelmed by alerts and repetitive tasks. They can perform difficult tasks such as analyzing massive amounts of data and triaging low-risk alarms so that humans can deal with the simple stuff.

Machine learning and AI in security is not yet up to standards today however in the future this can become something that can truly begin a new era of IT security. For cybersecurity today to reach new heights, machine learning and AI would have to have a good success rate with detecting anomalies by finding unusual patterns. Artificial Intelligence in cybersecurity might be harder to achieve depending on the rate of growth in the complexity of computing over the years. The usage of AI in cybersecurity systems will not mean complete immunity from hackers as it is most likely that AI systems will become a major target for hackers instead. Cybersecurity software in the future will be forced to create techniques to notice and counteract AI corruption attacks.

**What is the likely impact?**

As the internet of things (IoT) begin to increase, the surface area of vulnerable data and information at which hackers can infiltrate would also increase. Although large companies have much higher security and protection regarding their data, data breaches are still a common issue even for companies like Facebook and Twitch. The potential impact of the development of machine learning and AI within IT security is of course the decrease in cyberattacks that target large corporations in an attempt to steal and alter any sensitive information. The people most affected by this change in cybersecurity should be everyone as almost everyone is an avid user of the internet but speaking from an industrial perspective then it would be large corporations and their IT security teams. The reason it being the IT security teams is because automation of security countermeasures makes the jobs of IT security professionals much easier as all the difficult work would go to through the AI’s algorithm. There will not be any changes regarding the demand of cybersecurity developers and professionals as the AI system is merely a tool to address vulnerabilities and find security issues before it is too late so countermeasures can be activated in place.

**How will this affect you?**

As a frequent user of the internet, machine learning and AI in cybersecurity can be extremely helpful in preventing future cyberattacks however, the cost of a machine learning project can be quite expensive and not practical for the average internet consumer. The costs of AI or machine learning can cost from a few thousand to a few hundred thousand dollars. Large companies who choose to take machine learning and AI on board for cybersecurity’s sake will allow their consumers to be better protected against malicious malware and hackers. Cyber-attacks will never be eliminated due to the fact that 95% of successful cyberattacks are the result of human error however, companies can be more readily prepared to activate safety measures against potential data breaches by employing AI. We internet consumers already have various ways to protect ourselves against almost all types of cyber threats so not much will change regarding our cyber security as we are the sole ones responsible for any threats that we might fall for. The only thing that would change is obviously the level of security of large companies that we put our trust in safekeeping all our sensitive data. If machine learning and AI works successfully as a protection against cyber threats, then the public’s trust in the company would be substantially improved.

References:

Services, P., 2022. *What Is Cybersecurity?*. [online] Cisco. Available at: <https://www.cisco.com/c/en\_au/products/security/what-is-cybersecurity.html#~types-of-threats> [Accessed 1 May 2022].

Parker, J., 2022. *What is the future of cybersecurity?*. [online] TechRadar. Available at: <https://www.techradar.com/au/news/what-is-the-future-of-cybersecurity> [Accessed 1 May 2022].

The AME Group. 2022. *5 Trends That Advance Cyber Protection*. [online] Available at: <https://www.theamegroup.com/5-trends-advance-cyber-protection/> [Accessed 1 May 2022].

SailPoint. 2022. *How AI and Machine Learning Are Improving Cybersecurity*. [online] Available at: <https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity/#:~:text=AI%20and%20machine%20learning%20makes,attacks%20as%20new%20data%20emerges.> [Accessed 1 May 2022].

Perlman, A., 2022. *The Growing Role of Machine Learning in Cybersecurity*. [online] SecurityRoundTable.org. Available at: <https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/#:~:text=With%20machine%20learning%2C%20cybersecurity%20systems,active%20attacks%20in%20real%20time.> [Accessed 1 May 2022].

Linders, B., 2022. *What Machine Learning Can Do for Security*. [online] InfoQ. Available at: <https://www.infoq.com/news/2021/11/machine-learning-security/> [Accessed 1 May 2022].