**What is it?**

Cyber security is an extremely prevalent topic in the world of I.T. and has dramatically changed within the last two decades, as the internet has become integrated into most parts of modern day life. Cybersecurity technology is now being injected into almost anything that has direct communication to the internet to protect users from having their personal data compromised. To remain vigilant in the world of cyber cime, there have been many new technologies created to defend against hackers and intruders including Next-Generation Intrusion Prevention System (NGIPS), Firewalls, Advanced Malware protection systems, encryption/cryptography and intrusion detection systems. These will be explored in more detail below.

Firewalls. Firewalls were one of the earliest preventative measures developed for I.T systems. Firewalls would be designated filters and scan packets of information being transferred via a network connection. The firewall would search packets and would reject them if they did not meet the specifications of the filter, otherwise the packets were allowed through. The firewall has been vastly improved upon, with the integration of the application layer, allowing it to filter access for specified applications. Intrusion Detection Systems are similar to firewalls, but as a firewall looks outwardly for intrusions, an IDS signals a warning one the intrusion has taken place. The IDS monitors behaviour on a network and identifies anomalies and unusual behaviour before alerting the administrator to the suspicious activity.

A very important preventative measure in cyber security is the implementation of encryption and cryptography software. These applications allow data to be transmitted across the internet, through a public domain and remain unreadable to all but the render and receiver. One of the critical and commonly used methods is the Diffie-Hellman key exchange, which allows two users to share information securly. The two users have their own “key” and exchange information using a combination of their own key and a public key. The two parties are then able to decipher the secret. This method, and many similar protocols are implemented in almost every piece of software that connects to the internet. Every single website that shares information relating to a persons details, financial information, government information, and anything that could be considered sensitive or private, would utilise a similar protocol to communicate this data.

Preventative software such as anti-virus and anti-malware applications are very common and predominant on most computer systems, in which they are used to identify if a harmful piece of malware has been installed and then remove it. Malware is often designed to infect a machine so that its owner may steal or copy information stored on the machine, and even in some case, take control of the infected system. There are many types of viruses and therefore, many ways the anti-virus software can look for a piece of malware. These include, observing and evaluating a programs behaviour to identify if it is suspicious, using a database of “signatures” to see if it is a commonly known virus and monitoring data being loaded into the computers active memory.

All of these systems detailed have undergone many advancements and changes, particularly over the last two decades, as the rate of cyber crime has not only increased, but has become an every day occurrence. Cyber crime is now a constantly evolving part of the I.T industry, as technology is advancing, not only are security professionals integrating them into their existing systems, so are the cyber criminals. One of the newest technologies to be considered in the fight against cybercrime is machine learning, a concept that will utilise artificial intelligence algorithms to identify and prevent intrusions or malicious attacks.

**What is the impact?**

The implementation of machine learning into the cyber security field will most likely be a very positive addition. It will certainly make detection of threats much easier, and will assist current security analysts greatly. Its quite hard to determine what type of change this will have in relation to cyber security jobs. It's very unlikely to make jobs redundant, but will most likely require many hours of testing and refinement to accurately integrate machine learning into cyber security systems. Unfortunately due to the nature of cyber security, there will always be a need for security in the modern world, as there will always be criminals who wish to attack computer systems, whether it be for financial gain, the theft of information or secrets, identity theft, or something as simple as denial of services. It is safe to say that even as new technology is developed to prevent cyber crime, this same technology can be used to commit cyber crime.

**How will it affect you?**

The world has already changed so much due to the ever growing threat of cyber crime. Fortunately for most, as the introduction of new preventative cyber security measures become common, we will hopefully become more safe in the online realm. It is quite possible that we will have new systems or apps to guard our information, that will be integrated into our everyday devices. We already have many pieces of software that are commonly used such as antivirus programs and even software to help with passwords like Keychain Access. It is quite easy to predict that we will only have more and more programs available to use as new technology such as machine learning is refined and integrated into the cyber security field.