Three threats faced by technologies and the respective strategies used to secure them

Most people in the modern days cannot live without technology as it brings so many benefits to us. Modern technology changes the perceptions that people have of the world and the ways they act within the world (Tully C. J., 2003). Technology is necessary for most situations and strongly influences the procedures in young people's everyday lives, from leisure time to school to workplaces. People carry their small devices almost everywhere they go, to work, to study or for entertainment. Despite how people think of its positive influence, it also brings negative consequences if not used properly. This essay will now focus on three threats faced by technologies and the respective strategies used to secure them.

The first threat is malware. According to DuPaul N. (2012), malicious software, or malware, is used by cybercriminals, hackers to disrupt computer operations, steal data, bypass access controls and otherwise cause harm to the host system. There are many types of malware such as Trojan, Ransomware, Spyware and many more. Each type of malware have its unique traits and characteristics, for example a spyware is designed to collect information and the user's activity without the user's knowledge while a ransomware is designed to block the user from using the computer completely and ask for money to unlock it. Malware can be spread in many ways. They are usually spread on the internet via email and social media. The hacker will post a malicious link to the public on social media or send an email containing malicious attachments or links to random people in their contacts. When people click on the link or the attachment received from the hacker, the malware will infect the computer immediately. Malware can also be spread through advertisements. When browsing the internet, people tend to browse freely and click on anything that looks appealing to them such as advertisement. Most of the advertisement are legitimate product advertising, but there is some advertisement that can lead to malware. These advertisements are usually set to attract the most attention such as offers that are too good to be true. When people click on the advertisement they will most likely get an annoying popup, or a software containing malware downloaded to the computer without even noticing. Once the malware infected the computer, it can be a huge threat to the user as it can alter or delete files on the computer or even steal sensitive information from the computer depends on what type of malware it is.

The symptoms of a malware infected system is when the computer run slower than usual, unexpected crash or any other irregular activities. When these irregular activities occur on your computer, it is possible that your computer is infected by malware. The ideal way to prevent your computer from malware is to install antivirus software. Antivirus is a software that detects and eradicate malware from a computer system. Antivirus software works by scanning and running integrity checks to detect malware in the computer system. Once a file or folder is suspected of containing malware, the antivirus will quarantine the files to prevent them from harming the computer further. After that, the software will ask the user for permission to delete the malware infected files. Once permission is granted, the infected files will be deleted from the computer immediately. It is also important to realize which anti-virus software works best for your computer. A good example of antivirus software includes Windows Defender, Kaspersky, Norton and McAfee Antivirus. Also, make sure to run a virus scan on your computer daily as we do not know when and how the malware will infect the computer. If any symptoms of a malware

such as system crash occur to your computer, be sure to run the antivirus software scan immediately to remove the malware as quickly as possible before it can harm your computer. Hence, it is advisable that every computer or smartphone device should be equipped with antivirus software application and scan your device regularly to avoid malware infection.

Another threat is online identity theft. According to Mitchison N.(2004). Identity theft occurs when one person obtains data or documents belonging to another and then passes himself off as the victim. This credential information can be used to gain access to various things such as bank account and credit card details. Identity theft is usually done for financial gain, the thief who managed to get hold of the victim credit card can use it to make purchases and leaving the victim in huge debt. According to Collins A. (2017), more than 1 million kids had their identity stolen at cost of $2.6 billion in 2017. It is not very surprising that many kids got their identity stolen as they are still young and vulnerable to anyone convincing them to give information which could be used to get credit cards in the child's name. This does not mean that parents or old people who are knowledgeable can avoid this fully. There are many ways for the thief to obtain this information. The easiest way is through the internet. The thief can send an email impersonating the bank or a company asking you for your information. They can also obtain information through social media where people share their personal information like name, phone number and email through social networking sites such as Facebook, Instagram, and Twitter. Therefore, they can easily obtain other people personal information by just visiting their social media profile and gather all the information they need. Due to the users' carefree attitude in sharing information, social networking sites has become one the main target and the information available through social media can be used to attack even more sensible targets (Franchi E., Poggi A., Tomaiuolo M., 2017).

The easiest way to prevent this information from being stolen is to not share your personal information with the public on social media. Every social media platform has the option to hide sensitive information such as address, phone number and email from the public or only share with friends. Thus, all social media users should use this option to protect their information from hackers. Furthermore, only shop or give credentials information at reputable website. To check whether a website is trustable, check for the SSL certificate of the website. This can be done by looking at the URL of the website, if it begins with https instead of http means it is secured using SSL certificate. SSL certificate ensures that all your data collected by the website is sent straight from your browser to the website server with no middle person. It is not possible for a fake website or a scam website to get the SSL certificate. To get the SSL certificate, the website must go through a validation process. Therefore, it is recommended to not enter any credential information such as credit card details at website with URL starting with http as it is not secured by SSL certificate. Besides, if you get an email or a phone call from your bank asking for your account and passwords, they are most likely fake, a bank would never ask for account or passwords as it is already in their data. Therefore, do not give them any information. Hence, the key for protecting your data from being stolen is to not share it to the public and check carefully whether a website or the email sent to you is legitimate before entering any information.

Another threat is regarding cloud storage. For some computer users, having enough storage space to hold all their data is very challenging, they need to invest in external hard drive or thumb drive to be able to store all the data and need to carry around a physical device to access those data. This is where cloud storage comes in handy. Cloud storage is a service where data is remotely maintained, managed, and backed up. It allows the user to store files online so that the user can access them from any location via the internet without the need of

carrying any physical storage device. The provider company makes them available to the user online by keeping the uploaded files on an external server. This gives people using cloud storage ease and convenience. However, due to cloud storage being a third-party service, your data might be at risk of being viewed or accidentally leaked to others by the service provider. Hackers also will be able to access your files if they manage to get your account details or hack into the provider's system. As a result, your important data will be lost or accessed by other people without your permission.

The solution to this is to choose a good and trustable cloud service provider. The main reason to choose a trusted service provider is security. A good cloud storage service provider has a very high security system protecting the data, making it almost impossible for outsiders like hackers to gain access to the data without permission. Moreover, if your data happened to be loss, the company would be able to recover your files back to normal state and able to provide a compensation when such events happen. According to Good Cloud Storage (2018), the top 3 most secure cloud storage service providers are pCloud, Oracle and SpiderOak respectively. However, it depends on the user's preference whether security, accessibility or compatibility is the priority. Also, it is recommended to avoid storing sensitive data on the cloud. Personal details such as passport number and credit card details should not be stored on the cloud to ensure safety in case of data leakage. In addition, use a strong password for your account, avoid using your name or date of birth as it is easily guessable. A strong password should have a combination of numbers, symbols upper case letters, lower case letters and words not from dictionary to make it difficult for humans or even computer programs to generate your password. Fowler G. A. (2018) stated that password should be changed every 90 days and never, ever reuse a password. Thus, take your time to choose the best cloud storage service provider and be sure to use a strong password to increase the difficulty of others accessing your data.

In conclusion, technology has made people's lives better in many ways, it has become part of our everyday life. There are clearly both pros and cons of technology use. From when technology such as the internet was discovered until now, there are many threats related to it caused by human. Based on research findings, the proportion of cybercrimes is still growing constantly. This clearly shows that technology use cannot be controlled. It is predictable that in the future there will be even more threats that we will face from using technology. Therefore, it is important to have a good understanding of technology and we should know when and what to avoid when it comes to technology. Hence, we should not be overly dependent on technology, especially if you have very little knowledge about it. Technology is like the ocean, it can hold the boat, but also can sink the boat, so use it wisely.