Intro to IT: IT Technologies - Cyber Security

What does it do?

Cyber security is the idea of protecting online assets. The normal definition of security is to protect something, and this is the same thing but dealing with online clouds. Today, there is an ever-growing threat of cyber-attacks against anyone who uses the internet. There are many threats that people face online today such as malware attacks, trojan attacks and password breaches. The amount of information that is stored digitally has made cybercrime a large threat against corporate entities and individuals.

A way to counter these threats is to have a form of cyber security. There are many programs that protect the user from basic attacks such as windows defender. You can also purchase stronger protections like Norton. These programs are more designed for individual computers and not large companies. Larger companies typically employ a person that will protect their online information. Companies have more assets online with their drives including sensitive documents, so it is very common for them to have cyber security.

As the internet evolves and new programs are created, cyber security is also evolved around the ability to protect the newly designed programs. This means that cyber security is getting better every day and the firewalls and data encryption is being harder to breach.

Cybercrime has always been a problem in recent years and the attacks used can be summarised into 4 main ones. A malware attack can do many things to someone's computer, such as spyware and ransomware. One of the most notable recent ransomware attacks was the program 'WannaCry' that attacked hundreds of thousands of computers in 2017 (Fruhlinger, 2021). The malware attack will encrypt your files and then demand money for you to get them back. A spyware attack will pinpoint your location and key log your entries so they can steal valuable information from you. Another type of attack is online phone scams and email scams. This is where people will attempt to impersonate people or companies with promises of a package or money then take your money. These scams are quite prevalent in today's age, but the majority of people can see through the scam and not go through with it. This scam is more focused towards the elderly and young population who don't have much experience in dealing with these. Norton, Avast and Malwarebytes are some of the best anti malware programs out there. If you are not experienced with the internet and computers, the best way to protect yourself is to purchase these as they will protect you from most of the dangerous malwares.

Trojan viruses are also very common because they are very easy to trick people. The program will disguise itself as something the user wants such as a game or program but will put malware onto the person's computer. Most Trojan viruses are all the same but just disguises as different things and normally windows defender or any anti malware can pick it up. The best way to stop yourself against these attacks is to only download programs from official and trusted websites and by buying the program licenses rather than trying to burn them.

The role of a cybersecurity analyst is to prevent these cyber attacks that aim at the company they are working for. These cyber-attacks will commonly target sensitive information and try to extort money out of the company. A cybersecurity analyst will put measures in place that will prevent this from happening and in the unlikely scenario that it does happen, they will try to remove the malware and try and restore the lost data. This job will become harder each year because new malware is being created every week so the protection that stopped the last attack might not work on this new attack. The cybercriminals are becoming more advanced with finding ways to exploit the operating systems.

What is the likely impact?

As cyber security develops, it will create a safer environment for companies to store their information in clouds without the imminent risk of an attack. It will make the existing malware redundant as it is not longer useful against their defence. There are no negative effects of cybersecurity as it develops because it is in a totally new field of security. Everyone will still need physical security guards to protect physical things but on the internet, they will need cybersecurity. With the internet growing

every year, this will create more job opportunities for cybersecurity analysts as each company will need someone to help set up protective measures, so their information is safe.

If cybersecurity reaches a point in the future where a single program can protect itself against all malware attacks, then there may be a possibility of cybersecurity jobs becoming less sought after since a single program will be able to do everything. This possibility is not that realistic as malware cybercriminals are always finding new things that they can use against us. There are also many different programs and software that are built around specific companies which might be vulnerable to attacks. This means that cybersecurity jobs might be more flexible when dealing with different software and code.

There is also a concern of anti-malware programs collecting the user's information for data research. Since you are giving the program the whole administrative access to your computer, for them to defend it, they will need to scan through everything. This means there is no layer of protection that can protect against the Anti malware because that's its job to scan for threats. Although this might not be the case, it is something to think about with the whole recent issue of who is collecting your information.

How will this affect you?

With the advancements of cybersecurity, I believe this is a positive development because I would feel safer on the internet and downloading programs. Today, there is no way for a malware to force itself onto your computer, you must download it from the internet or through emails. This means that if you don't go anywhere sketchy, you will probably be no at risk. I feel like it won't really impact me on a personal level much as the other person because I have experience on the internet to know better than to download a trojan. Since I plan to go into the cybersecurity sector for work after university, I think the advancements will allow myself a higher job opportunity after graduating as the demand for cybersecurity is rising.

The recent developments of cyber security will affect my parents a lot more than me since they are not as experienced in the internet like myself. It will allow them to surf the web more without the risk of downloading a virus or getting a scam email which they might fall for. With my friends, I believe that this generation of people are generally more tech savvy and understanding of the present threats online. Cybersecurity will make the internet safer for everyone in general and has no real negative effects.

Bibliography

TechNewsWorld. 2021. The Future of Cybersecurity in 2021 and Beyond - TechNewsWorld. [online] Available at: <https://www.technewsworld.com/story/the-future-of-cybersecurity-in-2021-and-beyond-87018.html> [Accessed 9 September 2021].

Goddard, W., 2021. What is the Future of Cybersecurity?. [online] ITChronicles. Available at: <https://itchronicles.com/information-security/what-is-the-future-of-cybersecurity/> [Accessed 9 September 2021].

Fruhlinger, J., 2021. What is WannaCry ransomware, how does it infect, and who was responsible?. [online] CSO Online. Available at: <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html> [Accessed 16 September 2021].

Services, P., 2021. What Is Cybersecurity?. [online] Cisco. Available at: <https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html> [Accessed 16 September 2021].