**Beginning/inventors of cyber security**

Cyber security has come a long way with the steady rise of technological capability. Hackers hare targeting big companies such as google, or online banking sites to get valuable information.

There are 2.8 million cyber security jobs in the world according to a report published by (Jack Corrigan, 2019)**.** The research found the global shortage of cyber security workers increased by almost 40% over the past year which rose from 2.93 million vacant positions in 2018 to 4.07 million in 2019 which is over a million new vacant positions, this leaves major opportunities for computer science graduates.

1960’s Password Protection

In the 1960s businesses and organisations become more protective over information. There was no internet in the 1960 so business would try to stop people accessing data using passwords and multiple layers of security protection to try stop hackers accessing information. Information from companies may involve details of bank accounts or classified information from banks/ governments etc..

1970’s

Cyber security started in the 1970s when a research project was carried out by the ARPANET (the advanced research projects network). A researcher names Bob Thomas created a computer program which could move on ARPANETS network as it travelled across the network it left a small trail of messages wherever it went. The program was names “Creeper” which basically leaves printed messages when traveling across network. Ray Tomlinson the man who invented email created a next level “creeper” which was self-replicating and the first computer worm.

Tomlinson then created the program “reaper” which was able to chase the “creeper”, which was able to catch it and delete it, this was known as anti-virus software. Thomas and Tomlinson’s served highly important showing flaws in ARPANETS network.

People also began hacking phone lines or private lines created by organisations hackers began hacking phones lines to infiltrate these lines and steal information/data.

1980’s

Computers in the 1980s become more and more connected in ways people send and receive and store data. As computers get more and more connected and advanced hackers and viruses become more advanced.

In Russia when they began using cyberpower as a weapon in 1986 German computer hacker Marcus Hess was to steal US military secrets. Marcus hacked into over 400 computers including computers and mainframes at the Pentagon, they were going to sell their secrets to the KGB. He was then thwarted.

1998

In 1998 more people were using the network, more and more governments, colleges, business and militaries started using it.1998 was the year the worm was designed, it was designed to propagate across networks and to infiltrate terminals using a bug and copy of itself, it so identify lacking areas in a network intrusion prevention system.

Its downfall was the ability to self-replicate. It replicated itself so aggressively that it rendered targeted computers and slowed down the internet. During the 1980 ARPANETS network became known as the internet.

1990

In 1990 internet became available in most parts of the world, this meant that more and more people were putting their personal details online putting their details in danger of getting into the hand of hackers. firewalls and anti-virus programs were produced to try protecting the public from hackers.

Firewall was not as strong as it is today which meant hackers were sometimes able to get passed or into systems, in this period many hackers were getting away with light charges.

2000

In this period governments begin to clamp down on hacking by putting more serious charges on people who hack computers or systems. Virus’ start to become very dangerous as some virus’ can hack cities and even continents putting many people around the word at a danger.

2010

This is an era of some major breaches. Hacking is becoming more complicated as there is more security and harder security to hack that previous years.

Known as the first ‘ransomworm’, WannaCry hacked computers running the Microsoft Windows system and it asked for ransom payments in the Bitcoin cryptocurrency, it would demand payment. In only one day, the worm infected over 230 000 across 150 countries.

Edward Snowden a former CIA worker for the US Government who copied and leaked classified information from the National Security Agency, in the leaked information was evidence that the CIA were spying on the public. H was the most wanted man in the world and has still not been caught.

Hackers broke into Yahoo, releasing the accounts and personal information of all their three billion users. They were fined 35 million for this and yahoos sales dropped by 350 million.

These major data breaches drew a lot of attentions and made a lot of people angry, people should become more aware of what they are signing over on terms and condition of apps and websites , most apps take your personal details and can save and store your data. Tiktok has recently been accused of stealing and taking your data in which, it does. It also tracks your location if you have the app on your phone.

In conclusion we must stay protective over our data and personal information in the future as it can be hacked and looked at by various viewers.

References

# Jack Corrigan, 2019, Report: Cyber Workforce Must Grow 145% to Meet Global Demand, Nextgov, 1 May 2020. Available at:

<<https://www.nextgov.com/cybersecurity/2019/11/report-cyber-workforce-must-grow-145-meet-global-demand/161194/>>

* Dakota Murphy, Freeeline tech writer, 2019, a history of information security, IFSEC Global, 3 May 2020. Available at:

<<https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/>>