**THE EVOLUTION OF CYBERSECURITY**

           Since the inception of the internet, Cybersecurity has evolved immensely. Its historical development provides contexts for future references. Below is the chronological evolvement of Cybersecurity;

1. The Early Days (1960 - 1970s): In 1960; The creation of ARPAnet (Advanced Research Projects Agency Networks), the predecessor to the modern internet. The Creeper Virus, which was the first virus created by Bob Thomas in 1971, was a self-replicating virus which was harmless. It usually displayed “I’m the creeper, catch me if you can”. This was of main emphasis in the early days.
2. The Rise of Malware (1980s): in the year 1983, the term “Computer Virus” was created by Fred Cohen, while in the year 1986, the “Brain Virus” was created by two Pakistani brothers named Amjad & Basit Farouq Alvi which majorly targeted the MS-DOS booting sector of the computer, while in the year 1986, the Morris Worm was created by Robert Tappan Morris which gained a lot of media attention, caused a serious internet disruption and the likes.
3. Formalization of Cybersecurity (1990s) : In 1991, the first anti virus was created to fight the growth of malware threats, while in 1995, came a rise of phishing other online fraud, then came 1998 when the term cybersecurity became a widely used term and organisations such as “Computer Emergency Response Team (CERT)” was created.
4. The Age of Data Breaches (2000s): In the year 2000, the ILOVEYOUS virus was one of the most damaging viruses ever which spread across mails and caused billion dollars worth of damages, then came 2003, where the SQL slammer worm was created which disrupted MIcrosoft SQL servers in their vulnerable state. The Payment Card Industry Data Security Standard (PCI DSS) began to secure card transactions and information.
5. Advanced Persistent Threats and State Sponsored Attacks (2010s): Stuxnet, a sophisticated worm developed during cyber warfare. In 2013. Over 40 million customer’s personal and financial information was exposed which highlighted a huge vulnerability in retail security. In 206, DNC - Democratic National Committee’s email leaked attributed to Russian hackers.
6. Modern Cybersecurity Challenges (2020s and Beyond): 2020 came COVID-19 which called for robust security measures to be taken, while in 2021, the colonial ransomware attack disrupted fuel supply in the US and in 2023, the rise of AI began which enhances all fields and also put us at risk for more complex cyber attacks.

Cybersecurity and its scope is an ever growing phenomenon of study and it has the power to save humanity as it is.