**The objective of this mini project is to create a timeline highlighting the key events, technological advancement and pivotal moments in the evolution of cybersecurity.**

1. ***A TIMELINE SHOWCASING THE EVOLUTION OF CYBERSECURITY***

**1960s ---**-------**The beginning of cybersecurity**

* 1960s: the concept of computer security appears with mainframe computers. Passwords are introduced to restrict access.
* 1967: The first conference on computer security was held to discuss potential threats to emerging networks.

**1970s----------Early Cyber Threats**

* 1971: The first known computer virus, **creepe**r, was created as an experiment, displaying message as “IAM THE CREEPER. CATCH ME IF YOU CAN”
* 1972: The first antivirus program, called “REAPER” was created to remove Creeper
* 1976: Whitfield Diffie and Martin Hellman developed public-key cryptography, which revolutionized secure connection

**1980s--------- Rise of Malware& Cybercrime**

* 1983: the term **computer virus** was coined by Fred Cohen
* 1986: the **Computer Fraud and Abuse Act (CFAA)** was enacted in the U.S to address unauthorized access to computer
* 1988: the **Morris worm**, one of the first major worms, spreads across early internet, causing significant damage

**1990s---------- The Internet Boom &New Threats**

* 1991: the first commercial **antivirus** software was released
* 1994: the first **phishing attack** was recorded
* 1995: **JavaScript** was introduced, later leading to web-based cyber threats
* 1999: the **melissa virus** spreads through email attachments, causing widespread infections.

**2000s---------Cyber & Nation-State Attacks**

* 2000: the **ILOVEYOU** worm infected millions of computers via email
* 2001: the code **red worm** attacked Microsoft web servers
* 2003: the **SQL slammer worm** caused global internet slowdowns
* 2007: **operation Aurora**, a sophisticated cyber-attack on major companies like google, raises concerns about corporate espionage
* 2009: the **Stuxnet worm** was discovered, marking one of the first cyber weapons targeting industrial control systems

**2010s----------Ransomware &Advanced Threats**

* 2013: the **yahoo data breach** exposed three billion accounts, one of the largest breaches in history
* 2014: **Sony pictures hack** allegedly by North Korea, leaked sensitive data
* 2016: the **Mirai botnet** launched massive DDOS attacks, disrupting major websites
* 2017: the **WannaCry ransomware** attack affected 200000 computers worldwide
* 2018: the **Cambridge analytical scandal** revealed massive data privacy concerns
* 2019: **Magecart attacks** compromise e-commerce platforms through malicious JavaScript

**2020s---------- AI, Cloud Security, & Cyber warfare**

* 2020: the **Solarwinds attack** compromised multiple U.S government agencies
* 2021: the **colonial pipeline ransomware** attack caused fuel shortages in the U.S
* 2022: the **Log4j vulnerability** exposed critical systems to exploitation
* 2023: AI- driven deepfake scams and AI- powered cybersecurity solutions become a growing focus

1. ***TAKEAWAYS FOR CYBERSECURITY PRACTICES***

* Assume no network is safe, verify every user and device
* Use AI driven security tools for threat detection and incident response
* Educate users to prevent phishing and social engineering
* Employ firewalls, endpoint protection, intrusion detection, and encryption
* Follow CCPA, and Cybersecurity frameworks like NIST, ISO 2700. Cyber security practices have evolved from basic protection to AI-powered, protective, and intelligence- driven security frameworks

1. ***A PAGE VISUAL REPRESENTATION OF THE TIMELINE ON EVOLUTION CYBERSECURITY***

A group of colorful circles with arrows

AI-generated content may be incorrect.