Name: **Bashar Tukur Shehu**

Fellow ID: **FE/23/70792034**

Cohort: **Cohort 3**

Cyber Security Key Events from the earlier days of the internet

Year	Event	Description
1969	Creation of **ARPANET by the Pentagon's** Advanced Research Projects Agency.	The first ARPANET message was sent on Oct. 29, paving the way for more robust computer communication, greater vulnerability, and the eventual development of the Internet.
1971	Birth of Computer Virus/Worm - Creeper	Bob Thomas (a developer working for ARPANET) wrote a computer program that used PCs on the network to print the message: "**I'm the creeper; catch me if you can**." This was the first time a program moved from one computer to another on its own. The experiment was harmless, but in retrospect we can now say this was the first computer worm.
1972	Rise of the first Cyber Security program - Reaper	Fittingly, the advent of the first computer worm gave rise to the first cybersecurity effort to eliminate an unauthorized program. Ray Tomlinson - an ARPANET researcher who invented the first networked mail messaging system - developed a program named **Reaper**, which chased and deleted Creeper. Reaper was the very first example of antivirus software and the first self-replicating programme.
1983	Creation of the standardized **TCP/IP protocol** which lead to the birth of the internet.	TCP/IP became the global standard for network communications, allowing networks all over the world to communicate easily with each other. ARPANET and the Defense Data Network officially changed to the TCP/IP standard on January 1, 1983, hence the birth of the Internet.
1987	Spread of **Vienna virus**	In the late 80s, the **Vienna virus** destroyed random files on computers it infected. A simple virus with many known variants, it never did much damage and probably wouldn't have become famous except for one thing: it was stopped.

1987	Rise of the first Antivirus program	When German computer researcher Bernd Robert Fix received a copy of **Vienna**, he wrote a program that neutralized the virus' infective and destructive capabilities, making Vienna the first virus known to have been destroyed by an antivirus program.
1988	Internet Attack	Robert Morris, a 23-year-old graduate student from Cornell University, created and released several dozen lines of code that constituted the first Internet worm. The malware replicated wildly, infecting and crashing about 10% of the 60,000 computers connected to the internet and causing millions of dollars in damage.
1990's	Antivirus industry exploded	In the early 90s, the massive popularity of Microsoft's Windows operating system fueled a boom in the PC market—and an increase in virus activity. The antivirus industry responded with products like McAfee, Norton Antivirus and Kaspersky, which detected threats by scanning all the files in a system and comparing them to a database containing "signatures" of known malware.
1999	Mellisa Virus	Created by David Smith, this virus distributed itself via Microsoft Outlook. Infected computers would send an email with the subject "Important Message." and an attachment titled list.doc which, when opened, would cause a barrage of pornography sites to open. The virus would then disable security features in Word and Outlook, and mail itself to the first 50 people in the user's contact list.
2000	ILOVEYOU Worm	Infected more than 50 million Computers. This worm spread via an email with the subject "ILOVEYOU" and an attached file named "LOVE-LETTER-FOR-YOU.txt.vbs." When opened, a hidden script overwrote random files and sent a copy of itself to all of the addresses in the user's Outlook contacts. The infection spread so quickly that the Pentagon and the CIA shut down their email systems until the coast was clear.
2001	Fileless worm that evades antivirus detection	CodeRed spread via a buffer overflow, wherein a program writes too much data to the "buffer" section of memory, causing an overflow that overwrites adjacent memory locations. This allowed the worm to spread itself to other

		machines, and launch targeted DDoS attacks. Standard antivirus systems that scanned files to identify malware failed, as this worm was fileless.
2007	Birth of iPhone – A computer in every pocket	Apple launched the iPhone, giving every user a pocket-sized, internet-connected computer more powerful than the computer that landed Apollo 11 on the moon. Smartphones constitute a significant cybersecurity concern because the sheer number of them vastly increases the potential attack surface for a hacker to exploit.
2010	First weaponized malware program	Considered the first example of malware being weaponized on a global-scale, a sophisticated family of worms disrupted Iran’s nuclear program by interfering with centrifuges being used for uranium enrichment. One of the first instances of cyberattacks used in espionage.
2012	Antivirus puts big data to work	As traditional cybersecurity programs that identified potential threats based on their “signature” began to fail, the first “next-gen” antivirus software began using big data analysis to detect malware by taking a broad, holistic view of user behaviors, network traffic and application activity.
2013-1014	Largest Data Breach in History	Kicking off a period of cyberattacks of unprecedented scale, Yahoo suffered a breach that ultimately resulted in the theft of 3 billion users’ personal data, a $35 million fine by the SEC, and 40 consumer class action lawsuits. The best part? They wouldn’t report the breach until 2016.
2020	Rise of Connected Devices (IoT)	As of 2020, it’s estimated that there are roughly 6.8 internet connected (IoT) devices per person around the globe. As the amount of personal data becomes more and more available, cybersecurity concerns continue to grow.

With each subsequent technological development, the tension between black-hat and white-hat hackers continues to grow. Both sides are quick to adapt their methods to try to catch the other unaware.

Today, cybersecurity is an intricate field, encompassing everything from endpoint security to network defenses, and now, Confidential Computing. The threats have become more sophisticated, leveraging AI and machine learning, making proactive and advanced defense mechanisms essential.