**TOPIC: EVOLUTION OF CYBERSECURITY**

1. The Creeper Virus, the first computer virus, appeared in 1971.

🔹 A self-replicating program known as the Creeper Virus displayed the words, "I am the creeper: catch me if you can."

🔹 Lesson: Developed the first antivirus program, Reaper, by introducing the idea of malicious self-propagating malware.

1. The 1980s: The Emergence of Malware and Computer Worms

🔹 The first notable worm to spread over the internet and cause serious slowdowns was the Morris Worm (1988).

🔹 Takeaway: Draw attention to the weaknesses in early networks, which prompted the creation of security measures and the Computer Emergency Response Team (CERT).

1. 1990s: Encryption and Firewalls

🔹 Checkpoint Software established the first commercial firewall, Firewall-1, in 1993, laying the groundwork for network security.

🔹 Secure Sockets Layer (SSL) encryption was first deployed by Netscape in 1995 to safeguard online transactions.

🔹 Lesson: Encryption was required for safe online communication, and firewalls became a basic security tool.

1. Cybercrime and Regulations in the 2000s

🔹 2001: The Nimda virus and Code Red worm attacked thousands of computers globally.

🔹 2004: The first widespread phishing attacks used email scams to target users and banks.

🔹 Emergence of regulations: Data security compliance standards are established under the Sarbanes-Oxley Act (2002) and PCI-DSS (2004).

🔹 Lesson: As online dangers grew, cybersecurity became a corporate and regulatory priority.

1. The 2010s saw an increase in nation-state attacks and ransomware.

🔹 The first known cyberweapon, Stuxnet (2010), was designed to target Iran's nuclear facilities.

🔹 Ransomware Boom (2013–2017): Governments and businesses were disrupted by CryptoLocker, WannaCry, and NotPetya.

🔹 Cloud Security Growth (2015+): Security solutions evolved to safeguard dispersed data as cloud services grew.

🔹 Lesson: Ransomware became a significant financial danger when nation-states militarized cyber tools.

1. AI, Zero Trust, and Quantum-Safe Security in the 2020s

🔹 Zero Trust Model (2020+): Businesses change their access control to "Never Trust, Always Verify."

🔹 AI and Machine Learning in Cybersecurity: By employing AI to examine trends, threat detection becomes proactive.

🔹 Threats to Quantum Computing: To guard against future attacks, researchers are investigating post-quantum encryption.

🔹 Takeaway: With an emphasis on zero-trust security, cybersecurity is developing into a predictive, AI-driven discipline.

