**Name: Chibuike Chidozie Ikeh**

**Topic: The Evolution of Cybersecurity**

A journey from playful experiments to AI-driven defenses

**1971 – The First Computer Virus (Creeper Virus)**

🔹 The **Creeper Virus** was a self-replicating program that displayed the message: *"I’m the creeper: catch me if you can."*  
🔹 *Lesson:* Introduced the concept of malicious self-propagating software, leading to the first antivirus program, **Reaper**.

**1980s – The Rise of Computer Worms and Malware**

🔹 **Morris Worm (1988):** The first major worm to spread across the internet, causing significant slowdowns.  
🔹 *Lesson:* Highlighted the vulnerabilities in early networks, leading to the development of security protocols and the **Computer Emergency Response Team (CERT).**

**1990s – Firewalls and Encryption**

🔹 **First Commercial Firewalls (1993):** Checkpoint Software released **Firewall-1**, setting the foundation for network security.  
🔹 **SSL Encryption (1995):** Netscape introduced **Secure Sockets Layer (SSL)** to protect online transactions.  
🔹 *Lesson:* Firewalls became a fundamental security measure, and encryption was necessary for secure online communication.

**2000s – Cybercrime and Regulations**

🔹 **2001:** The **Code Red worm** and **Nimda virus** infected thousands of machines worldwide.  
🔹 **2004:** The first large-scale **phishing attacks** targeted banks and users via email scams.  
🔹 **Regulations emerge:** The **Sarbanes-Oxley Act (2002)** and **PCI-DSS (2004)** set data security compliance standards.  
🔹 *Lesson:* Cybersecurity became a regulatory and business priority as online threats increased.

**2010s – Rise of Ransomware and Nation-State Attacks**

🔹 **Stuxnet (2010):** The first known **cyber weapon**, targeting Iran’s nuclear facilities.  
🔹 **Ransomware Boom (2013–2017):** **CryptoLocker, WannaCry, and NotPetya** disrupted businesses and governments.  
🔹 **Cloud Security Growth (2015+):** As cloud services expanded, security solutions adapted to protect distributed data.  
🔹 *Lesson:* Nation-states weaponized cyber tools, and ransomware became a massive financial threat.

**2020s – AI, Zero Trust, and Quantum-Safe Security**

🔹 **Zero Trust Model (2020+):** Organizations shift to *“Never Trust, Always Verify”* for access control.  
🔹 **AI and Machine Learning in Cybersecurity:** Threat detection becomes proactive, using AI to analyze patterns.  
🔹 **Quantum Computing Threats:** Researchers explore **post-quantum encryption** to protect against future attacks.  
🔹 *Lesson:* Cybersecurity is evolving into a predictive, AI-driven field with a focus on **zero-trust security**.

