**\*\*Web 1.0:\*\***

Time Period: 1990 - 2005

Content Type: Static, read-only content

User Interaction: Limited, read-only, Minimal, passive

Technology used: HTML, CSS

Example Platforms: GeoCities, static websites

Security Concerns: Simple website hacks, data theft

Possible Attacks: Basic defacement, SQL injection

**\*\*Web 2.0:\*\***

Time Period: 2005 - 2015

Content Type: Dynamic, user-generated content

User Interaction: Interactive, collaborative, social

Technology used: HTML5, JavaScript, AJAX, APIs

Example Platforms: Facebook, YouTube, Wikipedia, Blogs

Security Concerns: Phishing, identity theft, malware

Possible Attacks: Phishing, cross-site scripting, social engineering

**\*\*Web 3.0:\*\***

Time Period: 2015 - 2025

Content Type: Semantic, machine-readable content

User Interaction: Intelligent interaction (AI-driven)

Technology used: AI, Machine Learning, Blockchain, Semantic Web

Example Platforms: Siri, Wolfram Alpha, Ethereum

Security Concerns: Data privacy, AI biases, crypto theft

Possible Attacks: AI manipulation, blockchain hacking, AI data poisoning

**\*\*Web 4.0:\*\***

Time Period: 2025 onward

Content Type: Personalized, context-aware content

User Interaction: Highly personalized, proactive, predictive

Technology used: AI, Big Data, IoT, Augmented Reality/Virtual Reality

Example Platforms: Smart assistants, smart homes

Security Concerns: IoT vulnerabilities, big data misuse, deep surveillance

Possible Attacks: IoT hacking, data surveillance, privacy erosion

**\*\*Web 5.0:\*\***

Time Period: Speculative/future phase

Content Type: Emotional, intuitive content, symbiotic

User Interaction: Symbiotic and neural integration, human-like interaction

Technology used: AI, Neural Networks, Brain-Computer Interfaces

Example Platforms: Brain-computer interfaces, empathetic systems

Security Concerns: Neurological data breaches, AI ethics

Possible Attacks: Neurohacking, emotional manipulation, emotional   
exploitation