

AI Agents, Faster Phones & Quantum Leaps: May 2026 Tech News Highlights

Technology · Answer Key · 7 Questions

1. What new requirement are governments, particularly the United States, pushing for regarding AI models before their public release in May 2026?

- A) Mandatory public beta testing
- B) Mandatory pre-release testing and regulation**
- C) Voluntary industry self-regulation
- D) Open-source code disclosure

2. Which major tech company unveiled 'Gemini Spark' at I/O 2026, described as an always-on AI agent?

- A) OpenAI
- B) Microsoft
- C) Google**
- D) Anthropic

3. Anthropic's advanced AI model, reportedly named 'Mythos,' exposed what critical issues in May 2026?

- A) New vulnerabilities in cryptocurrency exchanges
- B) Decades-old bugs in financial and infrastructure systems**
- C) Flaws in next-generation quantum encryption
- D) Weaknesses in global satellite communication networks

4. What significant advancement is expected in smartphone charging speeds by 2026, allowing phones to charge from 0-100% in under 10 minutes?

- A) Wireless charging over long distances
- B) Solar-powered charging pads
- C) 150W+ fast charging technology**
- D) Kinetic energy harvesting

5. Beyond emergencies, what new capability is satellite connectivity in smartphones expected to offer by 2026?

- A) High-speed internet browsing
- B) Two-way texting and calling in remote areas**
- C) Direct satellite TV streaming
- D) Interplanetary communication

6. In cybersecurity, what new attack surface is rapidly emerging due to the widespread use of 'Agentic AI' by employees and developers?

- A) Traditional firewall bypasses
- B) Advanced persistent threats (APTs)
- C) New network protocol vulnerabilities
- D) Unmanaged AI agent proliferation**

7. What evolving cyber threat involves deepfake audio, video, and synthetic identities being used as dangerous tools for fraud?

- A) Ransomware-as-a-Service (RaaS)
- B) Distributed Denial of Service (DDoS) attacks
- C) Phishing and social engineering
- D) Identity deception and synthetic fraud**