

Is Your Encryption Quantum-Safe?

3-Minute Security Check (Printable Checklist)

www.SpecterAI.ai

How to use: Spend 30-60 seconds per section. Mark what you find, then follow the action steps at the bottom.

1) Check #1 - Web Browser (TLS Certificate)

- Open any HTTPS site, click the lock icon, open Certificate/Connection details.
- If you see RSA-2048 / RSA-4096 -> quantum-vulnerable (public key).
- If you see ECDSA P-256 / P-384 -> quantum-vulnerable (ECC).
- If you see ML-KEM / Kyber (often hybrid) -> moving toward post-quantum key establishment.

Note: Most sites still show RSA or ECDSA today. This check is about visibility, not panic.

2) Check #2 - VPN (Key Exchange Matters)

- Open VPN settings: look for Security / Protocol / Encryption details.
- Identify BOTH: (a) Key exchange method and (b) Cipher.
- If key exchange includes ECDHE or RSA -> quantum-vulnerable key exchange/auth.
- AES-256 is strong, but AES-256 alone does NOT make the VPN quantum-safe.
- Watch for ML-KEM / post-quantum or hybrid key exchange options as vendors add support.

Mental model: Vault door (AES) is strong, but if the key exchange can be broken, the session key can be recovered.

3) Check #3 - SSH Keys (Dev / Admin)

- Show your public key (examples): cat ~/.ssh/id_rsa.pub or view id_ed25519.pub.
- If it starts with ssh-rsa -> quantum-vulnerable (RSA).
- If it starts with ecdsa -> quantum-vulnerable (ECC).
- If it starts with ssh-ed25519 -> quantum-vulnerable (ECC-based Curve25519).
- Plan for post-quantum signatures (Dilithium / SPHINCS+) as tooling support matures.

Tip: Until PQ SSH is mainstream, mitigate with short-lived certs, frequent key rotation, and tight access controls.

4) Check #4 - Organization Systems (Ask IT)

- What does our VPN use for KEY EXCHANGE (not just AES-256 for the cipher)?
- Are our code-signing certificates RSA or ECC? (If yes, quantum-vulnerable signatures.)
- Do our APIs/JWT/OAuth flows rely on RSA or ECC for authentication/signing?
- Have we done a quantum readiness assessment (inventory of RSA/ECC/DH usage)?

Red flag answer: "We use RSA-2048" without a roadmap to ML-KEM/ML-DSA.

Risk Check (How Urgent Is This?)

- HIGH RISK: government/military, banks, healthcare, or any data that must stay secret >10 years.
- MEDIUM RISK: enterprises with trade secrets, M&A, legal/consulting confidentiality.
- LOWER RISK: short-lived personal comms and transactional data (still monitor upgrades).

Key concept: Harvest now, decrypt later - adversaries can store encrypted traffic today for future decryption.

Action Steps (What To Do Next)

- Individuals: monitor PQ browser/TLS rollouts (often hybrid first).
- Individuals: use AES-256 for local file encryption, avoid RSA-based key wrapping when possible.
- Individuals: choose vendors that publish PQC roadmaps for VPN/TLS.
- Organizations: run a quantum readiness assessment (inventory TLS, VPN, SSH, code signing, APIs).
- Organizations: prioritize migration for long-lived sensitive data first.
- Organizations: set a migration plan and timeline (do not wait until the last minute).

Terms to Watch (Quick Glossary)

- **ML-KEM:** NIST post-quantum key establishment (Kyber).
- **ML-DSA:** NIST post-quantum digital signatures (Dilithium).
- **ECDHE / ECDSA / RSA / Diffie-Hellman:** quantum-vulnerable public-key families under Shor's algorithm.
- **AES-256:** symmetric cipher; quantum provides a quadratic speedup (still strong).