NS Filtering To Block Malware At The Network Level — Ch

Print and tick off. ~30 minutes for full setup.

Date completed: _____
Re-run this quarterly. Each pass takes about 12 minutes.

Beginner — do these in order

- [ ] **1. DNS filtering provider chosen + account created**
  NextDNS / Cloudflare / Pi-hole
- [ ] **2. Malware + phishing blocklists enabled**
  Security tab
- [ ] **3. Router DNS pointed to filtering provider**
  WAN / DHCP settings
- [ ] **4. Verified active via test.nextdns.io**
  Shows filtering provider
- [ ] **5. Blocked-domain test passed**
  internetbadguys.com fails
- [ ] **6. DoH configured on phones + laptops**
  iOS profile / Android Private DNS / Windows Encrypted DNS
- [ ] **7. Dashboard reviewed for first week**
  Confirm normal traffic
- [ ] **8. Whitelist exceptions added as needed**
  Site-by-site basis
- [ ] **9. Endpoint AV still active alongside**
  Layered defense

Advanced — if you want to go further

- [ ] Self-hosted Pi-hole + Unbound recursive
- [ ] Per-device profiles (kids vs adults)
- [ ] Category blocking (gambling, adult)
- [ ] AI-based threat detection enabled
- [ ] Force browsers to use specified DoH
- [ ] Block alternate DoH bypasses at firewall