Use DNS Filtering To Block Malware At The Network Level

in-English how-to. ~30 minutes. One setting that blocks malware, ads, and phishing across every device on your netw

Pick a filtering DNS provider, configure at the router, set up dashboards, test that it works.
Print, share, and re-run quarterly.

Do This Right Now

#	STEP
1.	Choose a provider: NextDNS / Cloudflare for Families / Pi-hole.
2.	Enable malware + phishing blocklists.
3.	Configure at the router for whole-network coverage.
4.	Verify with test.nextdns.io and internetbadguys.com.
5.	Set up DoH per mobile device for off-network protection.
6.	Monitor dashboard weekly initially.
7.	Whitelist legitimate sites that break.
8.	Keep endpoint AV running alongside.

Why This Matters

- DNS sits at the start of nearly every network operation. By filtering at the DNS layer, you block threats before they can transfer any pa
- Endpoint protection (Defender, etc.) works at the device level. DNS filtering works at the network level. They complement each other:
- Modern providers (NextDNS, Pi-hole, Cloudflare for Families, ControlD) maintain large block lists for known-malicious domains, phish