Low-Hanging IT Tune-Ups

Three quick, high-impact tweaks you can do today to tighten up your home or small-office setup — no toolbox, jargon, or caffeine overdose required.

DNS Settings

Set your DHCP scope or device DNS servers to **1.1.1.2** (for malware filtering) or **1.1.1.3** (for malware + adult content filtering). They're Cloudflare's privacy-focused DNS resolvers — fast, free, and quietly protective at the network layer.

Heads-up: If your router also hands out addresses to Verizon Fios or Comcast set-top boxes, don't flip this switch globally — your channel guide might vanish faster than your patience.

Wi-Fi Password Strength

If your Wi-Fi password is still the family pet's name... we need to talk. Weak or reused passwords are how most home networks get compromised.

Try **DinoPass.com** — it generates strong but memorable passwords that even non-tech folks can handle.

People laugh when I pull up DinoPass. I just grin and remind them — security doesn't have to be completely boring.

System Auto-Updates

It's easy to click "remind me later" — until "later" becomes ransomware Tuesday. Make sure Windows, macOS, and mobile devices all have **automatic updates enabled**. Unpatched systems remain the #1 way attackers get in.

If your router or firewall supports auto-firmware updates, turn those on too. Your future self will thank you (probably while sipping coffee during a crisis that never happened).

Why It Matters

These simple fixes close some of the biggest gaps we find during initial Co-IT assessments. They're fast, free, and way less painful than explaining to your staff why "GuestNetwork2020" wasn't such a clever password after all.

For deeper protection — and a lot less guesswork — grab your **Co-IT Resource Pack** at **https://www.enuclea.com/co-it-resources.php**

Quick Win Checklist

- Update DNS settings on primary devices
- Generate and deploy strong Wi-Fi passwords
- Enable automatic updates everywhere
- Test router firmware auto-update settings