Sentrly — Windows Cleanup Checklist

Maintenance and security pass for Windows machines — startup, updates, and storage.

Router & firmware

- ■ Change the router's default admin password to something unique and long.
  Default credentials are widely published and scanned for from the open internet.
- ■ Apply the latest firmware update from the manufacturer.
  Most routers support auto-updates — turn them on and confirm a recent install date.
- ■ Disable remote administration unless you actively use it.
  If the admin panel is reachable from the internet, every internet user is a potential attacker.
- ■ Disable WPS (Wi-Fi Protected Setup).
  WPS PIN authentication has known weaknesses; pairing by password is safer.
- ■ Disable UPnP if you don't run servers or game consoles that need it.
  UPnP lets devices punch holes in your firewall without your knowledge.

Wi-Fi

- ■ Set Wi-Fi encryption to WPA3, or WPA2-AES if WPA3 isn't available.
  Avoid WEP and WPA-TKIP — both are broken.
- ■ Use a passphrase of 14+ characters or 5+ random words.
  Wi-Fi passwords are guessed offline once an attacker captures a handshake.
- ■ Hide guest devices and visitors on a separate guest network.
  Guest SSIDs prevent visitors from reaching your internal devices and shares.
- ■ Disable 'allow guests to see each other' on the guest network.
  Most routers expose this toggle. Keep guests isolated from each other too.

Devices & IoT

- ■ Inventory every device on your LAN. Identify each one.
  Most routers have a connected-devices list. Anything you can't identify is a problem.
- ■ Enable automatic updates on phones, laptops, smart TVs, and consoles.
  The biggest gap on home networks is unpatched devices, not 'hackers in your router.'
- ■ Put smart-home and IoT gear on a separate VLAN or guest network.
  If your fridge gets compromised, it shouldn't reach your laptop.
- ■ Replace any device that no longer receives security updates.
  End-of-life routers, cameras and DVRs are common entry points.

DNS & filtering

- ■ Set encrypted DNS (DoH or DoT) on your router or each device.
  Encrypted DNS prevents your ISP and on-path observers from reading every domain you visit.
- ■ Add network-wide content filtering for malware/phishing domains.

Many free DNS resolvers offer this — Cloudflare 1.1.1.2, Quad9, NextDNS, AdGuard DNS.