Checkliste: WLAN absichern

1. Zugangsdaten & Passwörter

- ☐ Standard-Passwort des Routers geändert
- ☐ Starkes WLAN-Passwort eingerichtet (mind. 12 Zeichen, Sonderzeichen, Zahlen)
- ☐ Router-Login mit sicherem Admin-Passwort geschützt

2. Verschlüsselung & Sicherheitseinstellungen

- ☐ WPA3 aktiviert (alternativ: WPA2, niemals WEP oder unverschlüsselt)
- ☐ Gast-WLAN eingerichtet für Besucher (getrennt vom Hauptnetzwerk)
- ☐ SSID (WLAN-Name) individuell benannt, keine Standardnamen (z. B. „Fritz!Box1234“)

3. Router & Firmware

- ☐ Firmware regelmäßig aktualisiert
- ☐ Remote-Zugriff auf den Router deaktiviert (falls nicht benötigt)
- ☐ UPnP-Funktion (Universal Plug and Play) deaktiviert, wenn nicht zwingend notwendig

4. Netzwerk-Management

- ☐ Nur bekannte Geräte haben Zugriff (MAC-Filter optional aktiv)
- ☐ Kinder- oder Zeitprofile bei Bedarf eingerichtet
- ☐ Geräte im Heimnetzwerk regelmäßig überprüft

5. Erweiterte Sicherheitsmaßnahmen

- ☐ Firewall im Router aktiviert
- ☐ VPN genutzt, wenn ich von außen auf mein Heimnetz zugreife
- ☐ Backups meiner Router-Einstellungen gespeichert

Fazit

Ein sicheres WLAN schützt nicht nur deine Geräte, sondern auch deine persönlichen Daten. Mit dieser Checkliste stellst du sicher, dass dein Netzwerk optimal gegen Angriffe abgesichert ist.