Remote Worker Security Checklist

Network, device, and habit checks for anyone working from home — in one printable page.

From the TechODash Remote Work Security series. Work through it once, then revisit quarterly.

NETWORK

- ☐ **Work traffic runs through a VPN**
  Keep it active for anything work-related, especially on Wi-Fi you don't fully control.
- ☐ **Work devices sit on their own network segment**
  Use your router's guest network or a VLAN so a compromised smart device can't reach your work laptop.
- ☐ **Wi-Fi encryption is set to WPA3 (or WPA2 if unavailable)**
  Avoid WEP and original WPA entirely — both are obsolete and easily broken.

DEVICE

- ☐ **Full-disk encryption is turned on**
  Built into most modern operating systems — protects your data if the device is lost or stolen.
- ☐ **Screen lock and auto-lock are configured**
  A short auto-lock timeout matters most on a device that travels or sits in shared spaces.
- ☐ **Two-factor authentication is enabled on primary work accounts**
  Prefer an authenticator app or hardware key over SMS codes where the option exists.

HABITS

- ☐ **Unexpected payment or account-change requests get verified independently**
  Call a number you already have on file — never one provided in the message itself.
- ☐ **Public Wi-Fi is never used for work without a VPN active**
  Coffee shop and airport networks are shared, unencrypted, and easy to eavesdrop on.
- ☐ **Important files are backed up on a real schedule**
  A 3-2-1 approach — a working copy, a local backup, and an offsite or cloud copy — covers most real failure scenarios.