



Working Remotely & Securely

A practical guide to staying secure when working from home or on the move. One-page summary.

The 10 things to remember

- 1 Your home router is part of the workplace: change the default admin password and keep firmware updated.
- 2 Work stays on the work device or a dedicated profile, never a shared family computer.
- 3 Patch promptly, lock the screen every time you step away, and confirm disk encryption is on.
- 4 Treat every public Wi-Fi network as untrusted: prefer your phone's hotspot, or use the VPN.
- 5 Assume screens and calls in public can be seen and heard; use a privacy filter and keep specifics vague.
- 6 Report a lost or stolen device to IT immediately; speed is what keeps a loss from becoming a breach.
- 7 Never plug in unknown USB drives, and charge from your own plug, not public USB ports.
- 8 Company data lives only in approved storage: no personal email, personal drives, or unapproved apps.
- 9 Shred work printouts; household bins and recycling are not secure disposal.
- 10 Unique passwords, a password manager, and MFA everywhere; deny any MFA prompt you did not trigger.