Remote Work Security Guide

Remote work expands the attack surface beyond the corporate network. Home networks, shared devices, and public Wi-Fi introduce risks that require deliberate security measures. This guide covers the essentials for maintaining security while working from anywhere.

Key Points

- ✓ Always use a VPN when accessing company resources from outside the office
- ✓ Secure your home Wi-Fi: WPA3 encryption, strong password, updated firmware
- ✓ Never use public Wi-Fi for sensitive work without a VPN
- ✓ Keep work and personal devices separate — avoid using personal devices for work
- ✓ Enable full-disk encryption on all devices used for work
- ✓ Ensure your home router has the latest firmware updates
- ✓ Use a dedicated workspace where screens are not visible to others
- ✓ Lock devices when stepping away, even at home

Action Items

1. Change your home Wi-Fi password if it is still the default
2. Update your home router firmware this week
3. Verify your VPN is active before accessing any work resources
4. Set up a separate Wi-Fi network (or VLAN) for work devices
5. Enable "Find My Device" on all work laptops and phones

Quick Reference

Remote Work Security Stack: VPN (always-on) + Full-disk encryption + Screen lock + Updated OS + MFA
Public Wi-Fi Rules: VPN required. No banking. No credential entry. Use mobile hotspot as alternative.
Video Calls: Use virtual backgrounds, check what is visible on camera, mute when not speaking.