

Remote Working Security Checklist

The basics for staff working from home or on the move

1. Devices

- ☐ Disk encryption enabled
- ☐ Automatic updates on
- ☐ Anti-malware active
- ☐ Automatic screen lock
- ☐ Remote wipe available

2. Connections

- ☐ Router default password changed
- ☐ Home Wi-Fi uses WPA2/WPA3
- ☐ VPN for internal systems
- ☐ No sensitive work on open public Wi-Fi

3. Accounts

- ☐ MFA on email and cloud services
- ☐ No work accounts on shared devices
- ☐ Unique passwords / password manager
- ☐ Refuse unexpected sign-in prompts

7. When to Run This Check

- When someone starts working remotely
- When they change devices
- After any security incident
- At least once a year for every remote worker

4. Data Handling

- ☐ Files stored in approved locations
- ☐ Share links, not attachments
- ☐ Home printing collected and shredded
- ☐ No personal email for business data

5. Physical Security

- ☐ Lock screens when unattended
- ☐ Angle screens away in public
- ☐ Never leave devices visible in cars
- ☐ Household members do not use work devices

6. If Something Goes Wrong

- ☐ Know who to contact immediately
- ☐ Report phishing without blame
- ☐ Passwords and sessions revoked fast
- ☐ Contacts stored off the device



Scan for the full guide
itclub.work/knowledge-centre

Encrypt the device. Protect the account. Know who to call.

IT Club

Technology Intelligence — Plain-English guidance for business owners

<https://itclub.work/knowledge-centre>