

Basic cyber skills checklist for UK business owners

The government's 2026 skills research found 57% of UK businesses lack confidence in basic cyber skills. These are the nine tasks it measured, plus the one it left out. Tick each when it is genuinely done, not merely intended. Most are free and need no specialist. The tags show which map to the five **Cyber Essentials** controls.

THE NINE BASIC SKILLS

- | | |
|---|--|
| ☐ 1. Store data securely. Know where important data lives and who can reach it; strong unique passwords, MFA and device encryption (BitLocker / FileVault) on.
SECURE CONFIG | ☐ 2. Configure your firewalls. Device firewalls on; the router not on its factory admin password; no forgotten services open to the internet. FIREWALLS |
| ☐ 3. Detect & remove malware. Defender (or equivalent) running and updating on every device; know the signs; disconnect and call for help early. MALWARE PROTECTION | ☐ 4. Handle personal data safely. Collect only what you need; move it by permissioned link over https, never loose email attachments or unencrypted USB sticks.
DATA / UK GDPR |
| ☐ 5. Restrict what software can run. Everyone works in a standard (non-admin) account day to day; install only from official sources; remove what you do not use.
SECURE CONFIG | ☐ 6. Choose secure device settings. Change every default password; passcode/biometric on all devices, phones included; turn off features you do not use.
SECURE CONFIG |
| ☐ 7. Keep software updated. Automatic updates on everywhere; a monthly reminder for what cannot self-update; replace anything past end of life.
UPDATE MANAGEMENT | ☐ 8. Manage user accounts. One account per person; least access for the role; remove leavers promptly; review a few times a year. ACCESS CONTROL |
| ☐ 9. Back up your data. Three copies, two media, one off-site or offline. Test a real restore once a quarter — an untested backup is a hope, not a plan. NCSC GUIDE | ☐ 10. Plan for the bad day. One page: who to call, where the backups are, how to reach customers if email is down, the ICO's 72-hour breach clock. THE ONE IT MISSED |

Do this first → Turn on **multi-factor authentication (MFA)** everywhere it is offered, starting with email. Email is the account attackers want most — it is where password resets for everything else arrive — and MFA is the single control that most reliably defeats a stolen password. Free, minutes per account.

Nine skills → one standard.

These are, almost exactly, the five Cyber Essentials controls plus the NCSC Small Business Guide. Certification is free to work towards and increasingly required to win contracts.

Full guide: cyber-defence.io/insights
Cyber Essentials help: cyber-defence.io/services/cyber-essentials
Free to use, print & share · Reviewed
Sept 2026