

Small Business Cybersecurity Checklist

Plain-language basics from our Cyber101 series. Check off what you already do. Anything left blank is your to-do list.

Work through it with whoever handles your computers, email and accounts. Most items take minutes, not days.

01 Passwords

- ☐ Everyone uses a password manager (for work accounts at minimum).
- ☐ Every account has its own password. No reuse between sites.
- ☐ Email, banking and admin accounts have long passphrases.
- ☐ No passwords on sticky notes, in spreadsheets or in group chats.

03 Phishing

- ☐ Staff know the signs: urgency, odd sender address, unexpected attachment or link.
- ☐ Any request to change bank details or pay an invoice is confirmed by phone, using a number you already have.
- ☐ There is one clear person to report a suspicious email to, and no blame for reporting.
- ☐ Nobody enters a password from a link in an email. Go to the site directly.

05 Public Wi-Fi

- ☐ No banking, payroll or admin work on open café or hotel Wi-Fi.
- ☐ Use a phone hotspot or a trusted VPN when away from the office.
- ☐ Your business guest Wi-Fi is separate from the network your registers and office PCs use.
- ☐ The office Wi-Fi password is changed from the default and when staff leave.

02 Multi-factor login (MFA)

- ☐ MFA is on for email first. Email resets everything else.
- ☐ MFA is on for banking, payroll, domain/website, and cloud storage.
- ☐ An authenticator app or security key is used where offered, not only text codes.
- ☐ Backup codes are stored somewhere safe, not in the same inbox.

04 Updates

- ☐ Automatic updates are on for computers, phones and browsers.
- ☐ Routers, printers and other devices get firmware updates too.
- ☐ Your website, plugins and point-of-sale software are kept current.
- ☐ Devices that no longer get security updates are on a replacement list.

06 Backups

- ☐ Important files and systems are backed up automatically.
- ☐ At least one copy is offline or in a separate cloud account.
- ☐ A test restore is done every quarter. Last test: _____
- ☐ One named person owns backups: _____

07 Shared logins

- ☐ One person, one account. No shared “front desk” or “office” logins.
- ☐ Admin accounts are separate from everyday accounts and used only for admin work.
- ☐ Only people who need access to a system have it.
- ☐ When someone leaves, their access is removed the same day.
- ☐ After offboarding, any shared passwords they knew are changed.

08 Know what you have

- ☐ You have a list of your key accounts: email, domain, website, bank, payroll, cloud.
- ☐ The business owner, not only a vendor or ex-employee, controls those accounts.
- ☐ You know who to call for IT help:

! If you're hit

1. **Disconnect** the affected device from Wi-Fi and the network. Do not wipe it yet.
2. **Change passwords** for email and banking from a different, clean device, and check that MFA is still on.
3. **Call your bank** right away if money or payment details may be involved.
4. **Write down** what happened and when: messages, screens, amounts. Screenshots help.
5. **Get help** from your IT provider before restoring anything. You can report cybercrime at ic3.gov.

Our to-do list
