

Is your Microsoft 365 secure?

A 10-point checklist for small UK businesses. Ten plain-English checks, with where to look.

1 Multi-factor sign-in for every user

A stolen password alone should never be enough to get into your email. Multi-factor authentication (MFA) asks for a second step, such as a prompt in the Microsoft Authenticator app. The NCSC recommends turning it on for every important account.

- In the Microsoft Entra admin centre, go to **Entra ID > Overview > Properties > Manage security defaults**. It should say **Enabled**, unless you use Conditional Access policies instead.
- Under **Authentication methods > User registration details**, check that every person shows as registered for MFA.

2 Admin accounts kept separate and protected

An administrator account can change everything, so it is the account attackers want most. It should not be the account you use for everyday email and browsing.

- In the Microsoft 365 admin centre, open **Roles > Role assignments > Global Administrator**. Microsoft recommends fewer than five people in this role.
- Each admin should use a separate, named admin account with MFA, not their everyday mailbox, and never a shared login. Keep one emergency ("break glass") admin account stored securely.

3 Legacy authentication switched off

Older sign-in methods (such as basic authentication over POP, IMAP or SMTP) cannot do MFA, so they let attackers bypass it with just a password.

- Security defaults block legacy authentication. If you use Conditional Access instead, make sure a policy blocks it.
- In the Entra admin centre, open **Sign-in logs** and filter **Client app** by the legacy options. Anything still appearing, often a scanner or an old app sending email, needs moving to a modern method first.

4 SPF, DKIM and DMARC set up for your domain

These three DNS records prove that email claiming to come from your domain really does, which helps your mail arrive and makes it harder for fraudsters to impersonate you.

- Use any free DNS lookup tool on your domain: you should see one SPF record (a TXT record starting `v=spf1`) and a DMARC record at `_dmarc.yourdomain`.
- In the Microsoft Defender portal, go to **Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM** and check DKIM is **Enabled** for your domain. Once the DMARC reports look clean, move its policy on from `p=none`.

5 Mailbox auditing on, and no unexpected forwarding

A common sign of a compromised mailbox is a hidden rule that forwards or deletes mail. Auditing gives you a record of what happened if something goes wrong.

- Mailbox auditing is on by default in Microsoft 365. To confirm, an admin can run `Get-OrganizationConfig | Format-List AuditDisabled` in Exchange Online PowerShell; **False** means it is on.
- In the Defender portal, set the outbound spam policy's automatic forwarding to **Off** unless you need it, and ask each person to check **Outlook > Settings > Mail > Rules** for anything they did not create.

6 File sharing outside the business under control

OneDrive and SharePoint make sharing easy, which also makes it easy to share too much. "Anyone with the link" links can be forwarded to people you never intended.

- In the SharePoint admin centre, open **Policies > Sharing**. Unless you need open links, choose **New and existing guests** rather than **Anyone**, and set the default link to **Specific people**.
- If you do allow Anyone links, set them to expire after a set number of days.

7 Leavers removed and licences tidied

Accounts belonging to people who have left are a quiet risk: nobody notices if they are misused. They can also cost you money in unused licences.

- In the Microsoft 365 admin centre, open **Users > Active users** and check that every account belongs to a current person or a known shared mailbox.
- For leavers: block sign-in, then convert the mailbox to a shared mailbox if you need to keep the mail, and remove the licence. Check **Billing > Licences** for licences you pay for but don't use.

8 Backups and retention decided, not assumed

Microsoft keeps your data available, but deleted items are only kept for a limited time. If something is deleted by mistake, by a leaver or by ransomware, you need a way back. The NCSC advises backing up your important data.

- By default, deleted email can usually be recovered for 14 days, and files deleted from OneDrive or SharePoint for 93 days. Decide whether that is enough for your business.
- If not, set a retention policy in the Microsoft Purview portal or use a separate Microsoft 365 backup service, and test a restore once.

9 Devices kept up to date and protected

Most attacks rely on known weaknesses that updates have already fixed. A lost laptop or phone should not mean lost data.

- On each Windows PC, check **Settings > Windows Update** installs updates automatically, and that the device runs a supported version. Windows 10 reached end of support in October 2025.
- Check that the disk is encrypted (**Settings > Privacy & security > Device encryption**, or BitLocker), antivirus such as Microsoft Defender is on, and every laptop and phone locks with a PIN, password or biometric.

10 Everyone knows how to spot and report phishing

Phishing emails are how most account takeovers and invoice frauds start. A team that knows what to look for, and feels able to report a mistake quickly, is one of your best defences.

- Make sure everyone can use the **Report** button in Outlook, and knows they can forward suspicious emails to the NCSC at report@phishing.gov.uk.
- Agree a simple rule: any request to change bank details or make an urgent payment is checked by phone on a number you already hold, never one in the email. The NCSC's free *Top Tips for Staff* training takes under 30 minutes.

Would you rather we checked? The Clarwyn IT Security Review and Remediation covers these points and more, rated red, amber or green in writing, with the red items fixed once you approve: £249 for up to 10 users. See clarwyn.co.uk/packages.html or email hello@clarwyn.co.uk.