Microsoft 365 security checklist for growing businesses

Ten settings that stop most attacks on businesses of 20 to 500 people. Tick each one only when you have checked it, not when you think it is probably fine.

- [ ] **1. Multi-factor authentication on every account, enforced**

  Why it matters. Password-only sign-in is how most Microsoft 365 breaches start. 'Security Defaults' or Conditional Access must require MFA for everyone, including shared mailboxes that anyone signs into and the account your accountant uses.

  How to check. Entra admin center → Users → Per-user MFA shows nothing enforced? Then check Conditional Access for a policy requiring MFA for all users, with no broad exclusions.

- [ ] **2. Conditional Access instead of Security Defaults**

  Why it matters. Security Defaults are better than nothing but cannot distinguish a managed laptop in the office from a stolen phone abroad. Conditional Access lets you require a compliant device, block risky sign-ins and limit what unmanaged devices can do.

  How to check. Entra admin center → Protection → Conditional Access. You want a small set of enabled policies, not report-only ones from two years ago.

- [ ] **3. Legacy authentication blocked**

  Why it matters. Old protocols (POP, IMAP, SMTP AUTH, basic auth) bypass MFA entirely. Attackers scan for them.

  How to check. Conditional Access policy targeting 'Other clients' with Block, or confirm in Sign-in logs that no legacy protocol sign-ins succeed.

- [ ] **4. Admin accounts separated and reduced**

  Why it matters. One person signing into email with a Global Admin account means one phishing email compromises the whole tenant. Admins should have a separate account used only for admin tasks, with phishing-resistant MFA.

  How to check. Entra admin center → Roles → Global Administrator. Two to four accounts, none of them daily-use mailboxes, plus two break-glass accounts.

- [ ] **5. Email authentication: SPF, DKIM and DMARC**

  Why it matters. Without these, anyone can send email that appears to come from your domain. DMARC at 'quarantine' or 'reject' stops it and tells you who is trying.

  How to check. Check your domain at a DMARC lookup tool. SPF should end -all, DKIM should be enabled for Microsoft 365 in the Defender portal, DMARC should exist with p=quarantine or p=reject.

- [ ] **6. Anti-phishing, Safe Links and Safe Attachments turned on**

  Why it matters. Defender for Office 365 (in Business Premium) catches impersonation and malicious links after delivery. The default policies are weak; the 'Standard' preset is one click.

  How to check. Defender portal → Email & collaboration → Policies → Preset security policies → Standard protection: On.

- [ ] **7. Mailbox forwarding to external addresses blocked**

  Why it matters. The first thing an attacker does after getting into a mailbox is add a rule forwarding everything outside. Block automatic external forwarding tenant-wide.

  How to check. Defender portal → Anti-spam outbound policy → Automatic forwarding: Off. Then check Exchange for existing forwarding rules.

- [ ] **8. Every device encrypted, patched and managed**

  Why it matters. A lost, unencrypted laptop is a reportable data breach. Managed devices (Intune, Jamf, Kandji) enforce encryption, screen lock and updates, and can be wiped remotely.

  How to check. Intune → Devices: every company device enrolled and compliant. Compliance policy requires BitLocker/FileVault and a supported OS version.

- [ ] **9. Sharing and guest access under control**

  Why it matters. Default SharePoint and OneDrive settings allow 'Anyone' links that never expire. Guests added years ago still have access to Teams.

  How to check. SharePoint admin center → Sharing: 'New and existing guests' at most, links expire, default to 'People in your organisation'. Review guests in Entra quarterly.

- [ ] **10. Backups tested, not assumed**

  Why it matters. Microsoft 365 retention is not a backup. Deleted, ransomed or maliciously wiped data needs a separate copy you have actually restored from.

  How to check. Name the backup product, the last restore test date and who ran it. If you cannot, you do not have a backup.

Want it checked for you? The Security Health Check reviews all of this and more against Cyber Essentials and Microsoft best practice, with a scored report and a prioritised fix list. Fixed price £1,250, two days. hello@soliman.co.uk · soliman.co.uk/packages

© Soliman Consulting Ltd. Free to share and print.