MICROSOFT 365 SECURITY CHECKLIST

Is your Microsoft 365 as secure as you think?

10 questions every business owner should be able to answer.

Microsoft 365 runs the day-to-day of most small businesses: email, files, Teams and calendars. Microsoft keeps the service running, but how securely it's set up for your business is down to you.

This checklist from IT Consultancy, Services & Solutions Ltd helps you see where you stand. You don't need to be technical, and "not sure" is a perfectly useful answer.

> **How to use it:** read each question and tick the answer that's honestly true today. Then count your "Yes" answers and see where you stand on page 3. It takes about ten minutes.

1 Does everyone need more than a password to sign in?

Most Microsoft 365 break-ins start with a stolen or guessed password. Multi-factor authentication - a code or app approval on your phone - stops most of these, but only if every account has it, including the boss and shared logins.

Good looks like: every account, with no exceptions, uses multi-factor authentication, through Microsoft's security defaults or Conditional Access policies.

- [ ] Yes, everyone
- [ ] Not sure
- [ ] No

2 How many people have full admin access?

An admin account can change anything, read anything and lock everyone else out. The more people who have one, and the more it's used for everyday email, the bigger the target.

Good looks like: two to four named admin accounts, kept separate from day-to-day accounts and only used when needed.

- [ ] Yes
- [ ] Not sure
- [ ] No

3 Do you know which apps can read your email and files?

Every time someone clicks "Sign in with Microsoft" on a new app - a scheduling tool, an AI note-taker, a PDF converter - they may be giving it access to company data. Fake apps use the same trick to get in without a password.

Good looks like: staff can't connect new apps without approval, and the apps already connected are reviewed regularly.

- [ ] Yes
- [ ] Not sure
- [ ] No

QUESTIONS 4 TO 9

4 If someone broke into an account, would you know - and know what to do?

Microsoft 365 can flag a login from another country at 3am, but only if someone sees the warning. Then every minute counts.

Good looks like: alerts go to a named person, with a plan to block the account, sign it out everywhere and check what was changed.

- [ ] Yes
- [ ] Not sure
- [ ] No

5 Could someone quietly forward your email to an outside address?

Attackers often add a hidden rule that copies emails elsewhere, then wait for an invoice to intercept.

Good looks like: forwarding to outside addresses is blocked unless approved, and new mailbox rules are reviewed.

- [ ] Yes, it's blocked
- [ ] Not sure
- [ ] No

6 Can criminals send emails that look like they're from you?

Without the right settings on your domain, anyone can send email that appears to come from your address. Three records called SPF, DKIM and DMARC prevent this.

Good looks like: all three are set up on your domain, and DMARC is set to reject or quarantine fake emails rather than just monitor them.

- [ ] Yes
- [ ] Not sure
- [ ] No

7 Do you know what's being shared outside the business?

"Anyone with the link" shares in OneDrive and SharePoint can be forwarded on, and they often outlive the project or the person who created them.

Good looks like: sharing is limited to named people by default, and old external shares are reviewed regularly.

- [ ] Yes
- [ ] Not sure
- [ ] No

8 If a laptop or phone was lost, could you lock it and wipe your data?

Business email and files live on laptops, tablets and personal phones. If one goes missing, you need to remove company data quickly and know it was encrypted.

Good looks like: company devices are managed through Microsoft 365, encrypted, and can be locked or wiped remotely.

- [ ] Yes
- [ ] Not sure
- [ ] No

9 Do leavers, guests and unused accounts lose access?

Accounts for former staff, old suppliers or one-off guests are easy to forget - and nobody notices if someone else starts using them.

Good looks like: leavers are blocked on their last day, and unused and guest accounts are reviewed and removed every few months.

- [ ] Yes
- [ ] Not sure
- [ ] No

QUESTION 10 AND YOUR SCORE

10

Are you using the security features you already pay for?

Many Microsoft 365 plans include strong security tools that were never switched on, and settings drift as changes are made. Cyber insurers increasingly ask about these controls before they'll cover you.

Good looks like: you know what your licence includes, and your Microsoft Secure Score is checked and improved over time.

- [ ] Yes
- [ ] Not sure
- [ ] No

How did you do?

Count the questions where you ticked the first box.

✓ 9 to 10	You're in a strong position. Keep reviewing these settings as your team and Microsoft 365 change.
! 6 to 8	The foundations are there, but there are gaps worth closing before someone else finds them.
× 5 or fewer	Your Microsoft 365 may be more exposed than you think. A free health check is a sensible next step.

NEXT STEP

Book a free Microsoft 365 health check

Bring your completed checklist to a 20-minute call. Before we speak, we'll check your domain's email security settings from the outside - no access or passwords needed. Together we'll look at:

- your answers, and what they mean for your business
- what our outside check found
- the gaps that matter most, and practical ways to close them

www.uk-it.uk/booking

Scan to book

About us

IT Consultancy, Services & Solutions Ltd is an IT support company based in Tewkesbury, looking after businesses from one person up to around 50 staff across Gloucestershire, Worcestershire and beyond. We specialise in Microsoft 365, hold Cyber Essentials certification and bring over 20 years of IT experience. Prefer to talk now? Call 0330 223 0005 or email hello@uk-it.uk.