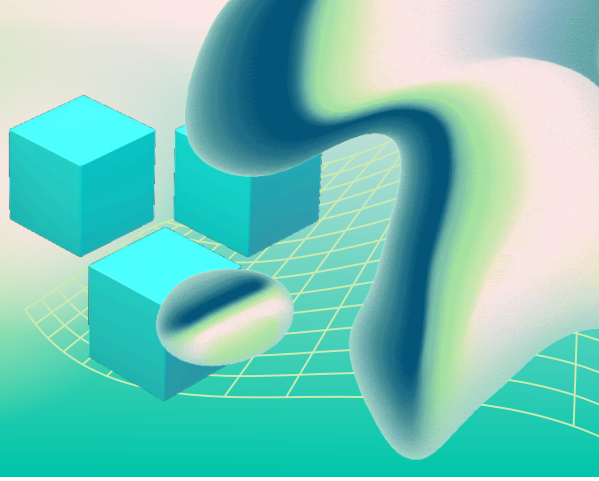
MS 365 SECURITY

Microsoft 365 is the core system for many small businesses—email, files, Teams, and identity all live in one place.



Microsoft 365 Security Checklist for Small Businesses (2026 Edition)

Use this checklist to verify your Microsoft 365 environment is set up for real-world security.

Microsoft 365 Security Checklist

1. Enforce Multi-Factor Authentication (MFA) for All Users

- ☐ MFA is required for every user
- ☐ Admin accounts use stronger MFA methods
- ☐ Legacy authentication (basic auth) is disabled

Why this matters:
Most Microsoft 365 breaches involve compromised credentials. MFA is the single most effective control.

2. Protect Admin Accounts Separately

- ☐ Admin accounts are separate from everyday user accounts
- ☐ Admin access is limited to only necessary users
- ☐ Admin activity is monitored

Why this matters:
Admin accounts provide full control. If compromised, the entire environment is at risk.

3. Use Conditional Access Policies

- ☐ Access is restricted based on location, device, or risk
- ☐ Unknown or risky logins are blocked or challenged
- ☐ High-risk users are flagged automatically

Why this matters:
Conditional access adds context to login decisions, reducing unauthorized access.

4. Enable Email Security Protections

□ Anti-phishing protection is enabled
□ Safe links and safe attachments are active
□ Spoofing protection is configured

Why this matters:
Email is the primary entry point for attacks in Microsoft 365.

5. Monitor Sign-In Activity and Alerts

□ Sign-in logs are reviewed periodically
□ Suspicious login attempts are investigated
□ Alerts are configured for unusual activity

Why this matters:
Early detection can stop an account takeover before damage spreads.

6. Secure OneDrive and SharePoint Access

□ File sharing is restricted to approved users
□ External sharing is limited or controlled
□ Sensitive files are not publicly accessible

Why this matters:
Data exposure often happens through misconfigured sharing, not hacking.

7. Use a Password Manager with Microsoft 365

□ Strong, unique passwords are used
□ Password reuse is eliminated
□ Credentials are stored securely

Why this matters:
Even with MFA, weak passwords increase risk.

8. Block or Limit Legacy and Unused Protocols

□ POP, IMAP, and legacy protocols are disabled where possible
□ Old or unused apps are removed
□ App access is reviewed regularly

Why this matters:
Legacy protocols bypass modern security controls like MFA.

9. Secure Devices Accessing Microsoft 365

□ Only approved devices can access company data
□ Devices are updated and protected
□ Mobile device access is controlled

Why this matters:
Microsoft 365 security depends on both identity and device trust.

10. Enable Data Loss Prevention (DLP) or Basic Controls

□ Sensitive data sharing is restricted
□ Policies prevent accidental exposure
□ Users are guided when handling sensitive data

Why this matters:
DLP reduces accidental leaks of sensitive information.

11. Configure Backup for Microsoft 365 Data

□ Email and files are backed up separately from Microsoft
□ Backup access is secured
□ Restore testing has been performed

Why this matters:
Microsoft 365 is not a full backup solution by default.

12. Train Employees on Microsoft 365 Security

□ Employees know how to spot phishing emails
□ Suspicious activity is reported quickly
□ Security practices are reinforced regularly

Why this matters:
Human behavior remains a key factor in account compromise.

13. Set Up Proper User Onboarding and Offboarding

□ New users are configured securely on day one
□ Departing users lose access immediately
□ Licenses and access are reviewed regularly

Why this matters:
Poor lifecycle management leads to unnecessary risk.

What a Secure Microsoft 365 Environment Looks Like

- **Every login is protected with MFA**
- **Admin access is controlled and monitored**
- **Email threats are filtered and reduced**
- **Data sharing is intentional—not accidental**

Quick Rule of Thumb

If one account can expose your entire system, your Microsoft 365 isn't fully secured.