FUSION1

FREE CHECKLIST · CYBERSECURITY BASICS

Microsoft 365 Security Checklist

Microsoft 365 includes strong security tools, but many are off by default or never configured. This checklist covers the settings we check first in every tenant we take over. If you're not sure where to look, that's worth knowing too.

How to use: Check only what you can confirm is in place today, then total your checks at the end.

1 Identity & sign-in

___ / 5

- [ ] **MFA is enforced for every user**
  Through Security Defaults or Conditional Access policies, not left up to each user.
- [ ] **Global Administrator is limited to a few dedicated admin accounts**
  Microsoft recommends fewer than five. Admins use a separate account for admin work.
- [ ] **An emergency access (break-glass) account exists and is secured**
  So a policy mistake or outage can't lock you out of your own tenant.
- [ ] **Legacy authentication protocols are blocked**
  Older protocols can bypass MFA.
- [ ] **Risky sign-ins and sign-ins from unexpected countries are reviewed or blocked**
  Conditional Access can restrict sign-ins by location and risk.

2 Email protection

___ / 5

- [ ] **Safe Links and Safe Attachments are enabled**
  Part of Microsoft Defender for Office 365, included in Business Premium.
- [ ] **Anti-phishing impersonation protection covers owners and finance staff**
  Flags look-alike senders pretending to be your leaders.
- [ ] **Automatic forwarding to external addresses is blocked**
  A common trick after an account is compromised.
- [ ] **SPF, DKIM, and DMARC are configured and DMARC is moving toward enforcement**
  A DMARC policy of 'none' only monitors; 'quarantine' or 'reject' actually protects.
- [ ] **Mailbox audit logging is on**
  You'll need it to investigate if something goes wrong.

3 Files & sharing

___ / 4

- [ ] **SharePoint and OneDrive external sharing is set deliberately**
  Not left at the most permissive default.
- [ ] **'Anyone' links are disabled or set to expire**
  Links that work for anyone who has them tend to spread.

- [ ] **Teams guest access is controlled**
  You know which outside people are in which teams.
- [ ] **Sensitive information is labeled or protected by data loss prevention (DLP)**
  Business Premium includes Purview Information Protection.

4 Devices

___ / 3

- [ ] **Company computers are enrolled in Intune (or another management tool)**
  Settings, updates, and encryption are enforced centrally.
- [ ] **Phones accessing company data have app protection policies**
  You can remove company data from a lost or personal phone without wiping the whole device.
- [ ] **Only compliant devices can access company data**
  Conditional Access checks device health before granting access.

5 Backup, monitoring & licensing

___ / 4

- [ ] **Exchange, OneDrive, SharePoint, and Teams are backed up by a third-party service**
  Microsoft's retention features are not a substitute for a backup.
- [ ] **Alert policies are reviewed and routed to someone who acts on them**
  Alerts nobody reads don't protect anything.
- [ ] **Microsoft Secure Score is reviewed at least monthly**
  It's a free, built-in to-do list for your tenant.
- [ ] **Licenses match what each person actually needs**
  Unused licenses are removed; key users have the security features they need.

Your score

Items checked: _____ of 21 = _____ %

90-100%
Strong
You have solid fundamentals. Review this checklist twice a year to keep it that way.

65-89%
Gaps to close
A good base with a few real exposures. Start with the unchecked items in the first two sections.

Below 65%
At risk
Several core protections are missing. Prioritize now, before an incident sets the agenda for you.