

Microsoft 365 security settings

The settings worth changing in a small business tenant, where to find them, and what each one affects if you get it wrong.

SETTING	WHERE TO FIND IT	WHY IT MATTERS	WHAT IT CAN AFFECT
Multi-factor authentication for every user	Microsoft Entra admin centre → Security defaults, or Conditional Access (Business Premium)	Stops a stolen password on its own from opening the account.	Staff need the Authenticator app set up first. Very old email apps and devices that cannot do MFA stop signing in.
Block automatic forwarding to external addresses	Microsoft Defender portal → Email & collaboration → Policies → Anti-spam → Outbound policy	Stops an attacker silently copying a mailbox to their own address.	Genuine forwards to outside addresses stop. Allow exceptions deliberately, per mailbox.
Separate admin accounts	Microsoft 365 admin centre → Users	Limits the damage if an everyday account is compromised.	Admins sign in with a second account for admin tasks.
Restrict “Anyone” sharing links	SharePoint admin centre → Policies → Sharing	Stops files being opened by anybody who gets hold of a link.	External people must verify who they are to open shared files.
Preset security policies for email	Microsoft Defender portal → Email & collaboration → Policies → Preset security policies	Applies Microsoft’s recommended anti-phishing and anti-malware settings in one step.	Occasionally a legitimate email is quarantined and needs releasing.
Audit logging	Microsoft Purview portal → Audit	Lets you investigate what happened after an incident.	Nothing — check it is on.
Security alerts to a monitored inbox	Microsoft Defender portal → Alert policies and notification settings	Makes sure someone sees warnings about suspicious sign-ins and forwarding rules.	Nothing.
Self-service password reset	Microsoft Entra admin centre → Password reset	Staff can reset forgotten passwords securely without waiting for an admin.	Users register a phone or app for verification.
Remove old accounts and spare licences	Microsoft 365 admin centre → Users / Licences	Closes forgotten ways in and stops paying for unused seats.	Convert leavers’ mailboxes to shared mailboxes first if you need to keep their email.

Before changing anything: tell staff what is happening, pick a quiet day, and make sure at least one administrator can still sign in if something goes wrong. Microsoft moves menus from time to time — the locations above were correct at the time of writing. Microsoft’s **Secure Score**, in the Defender portal, lists further recommendations for your tenant.