Lock Down Your Microsoft 365

A plain-English security guide for small-business owners

A free guide from PCA Technology Inc.

Nine things to check, in plain English, with steps you can follow in Microsoft's admin pages.

Edition: November 2026. Checked against Microsoft's published documentation on 27 November 2026.

pca-tech.com

Contents

Read this first 2
1. Turn on multifactor authentication for everyone, administrators first 4
2. Keep administrator accounts few, separate and recoverable 6
3. Block old sign-in methods that skip MFA 8
4. Protect against phishing and people pretending to be you 9
5. Find and block hidden mailbox forwarding 11
6. Keep file sharing under control in SharePoint and OneDrive 13
7. Cover the device basics 14
8. Know what is backed up, and for how long 16
9. A 20-minute check to do every month 17
The one-page checklist 19
Want the checking done for you? 20

Read this first

Many break-ins to a small business's Microsoft 365 do not involve clever hacking. Someone guesses or steals a password, signs in as your employee, and nothing stops them. Once inside, they read email, set up quiet rules to watch your invoices, and send believable messages to your customers.

The fixes are mostly settings you can check in an afternoon. Microsoft's own research says multifactor authentication (a second step when someone signs in) can block more than 99.2% of account-compromise attacks. This guide walks you through that and eight other things worth checking, in order of how much they matter.

How each chapter works

- Why it matters, with an example from an ordinary office.
- What good looks like, in one or two sentences.
- How to check this yourself, in numbered steps you can follow in the admin pages.
- Where your Microsoft 365 plan makes a difference, because some tools are free and some are not.
- A short note on where PCA Security Check fits. It is an automated, read-only scan that we sell. It is mentioned only where it genuinely helps, and each note says what it does not cover.

> **Examples are illustrations**
>
> The people in the examples (Dana, Marcus and the rest) are made up to show how these problems look in a 10-person office. They are not real cases or real customers.

What you need before you start

- A sign-in with an administrator role. Owners usually have Global Administrator by default, which can do everything in this guide. Where a smaller role is enough, the steps say so.
- About 15 to 30 minutes per chapter to check. Fixing can take longer.
- A note-taking habit. Write down every setting you change, the date, and the old value.

Which Microsoft 365 plan do you have?

Your plan decides which tools you have. To see it: sign in to the Microsoft 365 admin center, then open Billing and select Your products. The table below covers the three business plans most small offices use.

	Business Basic / Business Standard	Business Premium
Sign-in protection	Security defaults (free). On or off, no fine tuning.	Conditional Access (Microsoft Entra ID P1). Microsoft says security defaults are probably not right for organizations with P1.
Email protection	Built-in protection for every mailbox: anti-malware, anti-spam, spoofing protection	Everything in the left column, plus Microsoft Defender for Office 365 Plan 1: Safe Links, Safe Attachments and impersonation protection
Device management	Basic Mobility and Security (free; mainly for phones and tablets, limited for Windows PCs)	Microsoft Intune and Microsoft Defender for Business

If your plan sits on the left but you want the right-hand tools, ask your Microsoft reseller about add-ons: Microsoft documents that Conditional Access can also come from an add-on subscription. If you do not know which plan you have, the Your products page will show it.

Where to sign in

Admin center	Address	You will use it for
Microsoft 365 admin center	admin.microsoft.com	Users, admin roles, billing, domains
Microsoft Entra admin center	entra.microsoft.com	Sign-in security: MFA, security defaults, Conditional Access, guests
Microsoft Defender portal	security.microsoft.com	Email protection, Secure Score, email authentication
Exchange admin center	admin.exchange.microsoft.com	Mailboxes and mail flow reports
SharePoint admin center	From the Microsoft 365 admin center (select Show all if you do not see it)	File sharing settings

> **Before you change anything**
>
> 1. Change one thing at a time and write it down. 2. Where a step affects sign-in, keep a second administrator signed in on another device while you test, so one mistake does not lock everyone out. 3. Read Chapter 2's emergency-account section before turning on any rule that blocks or restricts sign-in. 4. Microsoft renames menus from time to time. If a name is slightly different, search for it in the admin center's search box.

1. Turn on multifactor authentication for everyone, administrators first

Why it matters

A password alone is one guess, one phishing page or one reused password away from being someone else's. Multifactor authentication (MFA) adds a second proof, usually a tap on a phone app, so a stolen password is not enough.

> **A familiar story (illustration)**
>
> Dana runs the front desk at a 10-person accounting office. She reuses one password on a few sites. One of them is breached, and the list ends up online. Nothing at the office is hacked. A stranger types Dana's email address and her old password into the Microsoft sign-in page. With MFA on, the sign-in stops there. Without it, the stranger is in Dana's mailbox before lunch.

Administrators matter most. An admin account can change settings for the whole company, so it should be the hardest to take over.

What good looks like

- Every user, and every administrator, has to complete MFA when they sign in.
- Administrators are covered first, and if possible by a phishing-resistant method such as a passkey or security key.
- You can see who has actually registered a second method, not just who has been told to.

Know what Microsoft already does, and what it does not

Microsoft requires MFA for sign-ins to its admin portals. Enforcement for the Microsoft 365 admin center began gradually from February 2025, and Microsoft requires it for the Azure portal, the Microsoft Entra admin center and the Microsoft Intune admin center as well. That protects the control room. It does not protect everyday email, files and Teams for your staff. For that you need your own setting.

You have two ways to do this, depending on your plan:

	Security defaults	Conditional Access
Plans	Available in all Microsoft 365 organizations (Microsoft Entra ID Free)	Needs Microsoft Entra ID P1 or higher, included in Business Premium
Cost	Free	Included in the plan, or an add-on
Control	On or off. No exceptions or tuning.	Fully customizable
What it does	Requires every user to register for MFA, requires admins to do MFA, blocks legacy sign-in protocols, and protects Azure management sign-ins	You build the rules. Microsoft provides templates such as Require multifactor authentication for all users and Require multifactor authentication for admins

	Security defaults	Conditional Access
Best for	Organizations on the free tier that want a basic level of protection without tuning	Offices that need exceptions, location rules or device rules

You cannot run both at once. Microsoft says to turn security defaults off only when you are switching to Conditional Access policies. If you turn it off and put nothing in its place, you are less protected than before.

> **Old per-user MFA**
>
> Microsoft calls the older per-user MFA setting 'legacy' and does not recommend it. If your tenant was created after 2019, it is probably not in use. If you do find it in use, treat moving to security defaults or Conditional Access as a project, not a quick toggle.

How to check this yourself

1. Sign in to the Microsoft Entra admin center (entra.microsoft.com) as at least a Conditional Access Administrator.
2. Go to Entra ID, then Overview, then Properties, and scroll to Security defaults.
3. Read what it says. 'Your organization is protected by security defaults' means security defaults are on. If it says your organization is using Conditional Access policies, security defaults is not available, because at least one Conditional Access policy exists. That policy may be Off or Report-only, so check in step 4 that the policies are really On. If it says 'not protected by security defaults', and you have no Conditional Access policies, you need to fix this now.
4. If you have Conditional Access (Business Premium), go to Entra ID, then Conditional Access, then Policies. Look for a policy that requires MFA for all users and another for administrators. Both should be set to On. A policy set to Report-only watches and logs but does not enforce anything.
5. To see who has registered a second method, ask each person to open myprofile.microsoft.com and choose Security info, or, as an admin, go to Entra ID, then Users, pick a person, and choose Authentication methods. With Entra ID P1 or P2 you also get a summary at Entra ID, then Authentication methods, then Activity, with a count of users capable of MFA.

If something is not right

- Security defaults off and no Conditional Access: on a free-tier plan, set Security defaults to Enabled and select Save. Tell your staff first, and check first whether a scanner, copier or old app sends email with a password, because security defaults blocks that (see Chapter 3). Once it is on, people are required to register for MFA with the Microsoft Authenticator app, and sign-ins that need it will prompt them.
- Business Premium: create the policies from Microsoft's templates. In Entra ID, Conditional Access, Policies, select New policy from template and, on the Secure foundation tab, choose Require multifactor authentication for all users and Require multifactor authentication for admins. Turn security defaults off first, because the two cannot run together. Before you create anything, look at the Created by column on the Policies page: Microsoft may already have added policies of its own, such as 'Multifactor authentication for all users' and 'Block legacy authentication'. They start in Report-only, and Microsoft turns them on no sooner than 30 days after they appear unless you turn them on or off yourself. On the Review + create tab set Policy state to On. Microsoft pre-excludes the account you are signed in with, so

afterwards open each policy, go to Users, then Exclude, remove yourself, and leave only your emergency access accounts (or their group). Do the same exclusion check on any Microsoft-created policy you switch on.

- Admins: Microsoft recommends going one step further and requiring phishing-resistant MFA, such as a passkey (FIDO2 security key), for administrators. Make sure every admin has registered one before you turn that policy on, or you can lock yourself out.
- If your staff sign in with text-message or phone-call codes: Microsoft is retiring its own SMS and voice MFA codes. Its FAQ says passkeys are being enabled automatically for users currently enabled for SMS or voice, and that the retirement applies to all users except Global Administrators and external users from 1 February 2027, and to Global Administrators and external users from 1 July 2027. Plan a move to the Microsoft Authenticator app or a passkey.
- Do not disable sign-in methods for your organization while security defaults is on. Microsoft warns this can lock you out of your own tenant.

Where PCA Security Check fits

PCA Security Check checks whether basic sign-in protection is switched on (security defaults or your own policies), whether administrators must use a second sign-in step and have registered one, and whether everyone must use one, including the share of staff who have registered. It reads your settings, and which sign-in methods each person has registered, and changes nothing. An administrator approves read-only access, and the report is emailed to that administrator. $199 for up to 50 users.

2. Keep administrator accounts few, separate and recoverable

Why it matters

Administrator accounts are the keys to everything. The more people who hold them, and the more they are used for everyday work, the more chances an attacker has.

> **A familiar story (illustration)**
>
> Marcus, the office manager, is the Global Administrator because he set up the account years ago. So is the former IT contractor, whose access nobody removed. Marcus reads email and clicks links all day on the same account that can change every setting. One bad click and the attacker holds the master key. Meanwhile, when Marcus is on holiday and the phone he uses for sign-in is lost, nobody can get in to fix anything.

What good looks like

- Fewer than five Global Administrators. Microsoft recommends this explicitly, and says all of them should be protected with MFA.
- People who only need to do one job get a smaller role (for example, someone who resets passwords does not need Global Administrator).

- Administrators use a separate account for admin work and another for everyday email and browsing. Microsoft recommends separate accounts for administration and for standard productivity tasks.
- Two emergency access ('break-glass') accounts exist, in case normal admin sign-in fails.
- Nobody is an administrator who no longer works for you or no longer needs it.

Emergency access accounts, in plain terms

An emergency access account is a spare administrator login that you set up and then store safely. You hope never to use it. It exists for the day normal admins cannot sign in: a lost phone, a mobile network outage, a mistaken policy that locks everyone out.

Microsoft's guidance is to create two or more of these, as cloud-only accounts on your *.onmicrosoft.com domain (not tied to a person, and not synced from any on-premises system) and give them the Global Administrator role. Key points from Microsoft's guidance:

- Use a different sign-in method from your regular admins. Microsoft recommends a passkey (FIDO2 security key). If your regular admins use the Microsoft Authenticator app, the emergency account should use something else.
- Store the credentials safely, such as in a fireproof safe, and in separate locations.
- Exclude them from any Conditional Access policy that blocks or restricts sign-in, including policies Microsoft creates for you on Business Premium (see Chapter 1). Microsoft suggests a dedicated security group for this. Report-only policies do not need an exclusion.
- Watch them. Microsoft's example sets up an alert for every sign-in by these accounts using Azure Monitor, which needs an Azure subscription and a Log Analytics workspace, so ask your IT provider to set it up. Test the accounts at least every 90 days.
- Do not use them for everyday work.

> **A note on MFA**
>
> Microsoft's mandatory MFA for its admin portals applies to emergency access accounts too, so a break-glass account must be able to complete MFA. That is why Microsoft recommends a passkey or certificate-based sign-in for these accounts, not a password and a phone.

How to check this yourself

1. Sign in to the Microsoft 365 admin center (admin.microsoft.com).
2. Go to Roles, then Role assignments. Select Global Administrator and look at the Assigned tab. Count the names. For a full list across all roles, use Export admin list.
3. For each name, ask: Is this a current employee? Do they need this level of access? Is this a person's everyday account? If a name fails any of these, change the role (Users, Active users, select the person, then Manage roles) to the smallest role that does the job.
4. Look for emergency access accounts. Check that there are at least two, that they are cloud-only on your onmicrosoft.com domain, that they have a different MFA method from your regular admins, and that someone knows where the credentials are stored.
5. Check in the Microsoft Entra admin center, under Entra ID, Overview: Microsoft shows a Global Administrators alert card there when you have five or more Global Administrator role assignments.

If something is not right

- Too many Global Administrators: remove the role from anyone who does not need it. Microsoft's own advice is to keep Global Administrator for emergencies and for tasks that smaller roles cannot do.
- No emergency accounts: create them before you turn on any new sign-in restrictions. Microsoft's article 'Manage emergency access accounts in Microsoft Entra ID' has the full steps.
- An ex-employee still holds a role: remove it today, and also check their account for sign-in activity and email forwarding (Chapter 5).

Where PCA Security Check fits

PCA Security Check counts how many people hold top-level administrator rights and flags too few or too many (it expects 2 to 4). It does not check whether your emergency access accounts exist, so use the steps above for that.

3. Block old sign-in methods that skip MFA

Why it matters

'Legacy authentication' means older ways of signing in that cannot ask for a second step: very old Office versions, and apps that use older mail protocols such as IMAP, POP and SMTP with just a password. Microsoft says most compromising sign-in attempts come from legacy authentication, and that an attacker can use an older protocol to bypass MFA even if you have turned MFA on.

> **A familiar story (illustration)**
> The office has MFA on. But the multifunction scanner in the corner sends scans to email using an old setting that needs only a username and password. An attacker who has one stolen password tries that old path. MFA never gets asked.

What good looks like

- Legacy authentication is blocked, either by security defaults (free) or by a Conditional Access policy.
- Nothing important still depends on it. If a device or app does, it is moved to a modern method.

Good news, and one thing still open

Microsoft has already switched off Basic authentication for most Exchange Online protocols in all tenants: Exchange ActiveSync, POP, IMAP, Remote PowerShell, Exchange Web Services, Offline Address Book, Autodiscover, and Outlook for Windows and Mac. It also disabled SMTP AUTH where it was not in use. SMTP AUTH is the one still open. Microsoft's updated timeline (January 2026) says: Basic authentication for SMTP AUTH stays as it is until the end of December 2026, when it will be disabled by default for existing tenants (administrators can still turn it on), and Microsoft will announce a final removal date in the second half of 2027.

In practice: if you have a scanner, copier, alarm system or old line-of-business app that sends email with a password, it is using SMTP AUTH. If security defaults is on, Microsoft says SMTP AUTH is already disabled, so that device will not work today. If you are not using security defaults, it keeps working until the end of

December 2026, when Microsoft disables it by default for existing tenants. Either way, move anything that sends mail to a modern method now.

How to check this yourself

1. Is security defaults on? See Chapter 1. If yes, legacy authentication is already blocked for you.
2. If you use Conditional Access, go to Entra ID, then Conditional Access, then Policies, and look for a policy named like 'Block legacy authentication' with Grant set to Block access. It should be On.
3. To see whether anyone still uses legacy sign-in, go to Entra ID, then Monitoring and health, then Sign-in logs. Add the Client app column, then use Add filters, Client app, and choose the legacy protocols. Select Apply. Repeat the same filter on the User sign-ins (non-interactive) tab, where many mail apps appear. Any rows are sign-ins by old methods. Each one tells you which user and which protocol.
4. Make a short list of anything that sends mail on its own (scanners, copiers, alarm panels, accounting software) and ask each vendor how to move it to a modern method.

If something is not right

- Business Premium: create a Conditional Access policy to block legacy authentication, using Microsoft's template or Microsoft's steps. Microsoft suggests starting in Report-only mode to see what it would affect, then switching it On.
- Free plans: security defaults blocks legacy authentication for you. Check the warning on Microsoft's page first: before enabling security defaults, make sure your administrators are not using older authentication protocols.

Where PCA Security Check fits

PCA Security Check checks whether old-style sign-in methods that skip the second step are blocked, and whether text-message and voice-call sign-in is limited. It does not look at individual devices such as scanners, so ask your vendors as described above.

4. Protect against phishing and people pretending to be you

Why it matters

Phishing is a message designed to trick someone into signing in on a fake page or sending money. There are two sides to it: fake mail pretending to come from you, and fake mail aimed at your staff.

> **A familiar story (illustration)**
> A customer receives an invoice that looks like it came from Marcus, with new bank details. It did not. Anyone can make a message look like it came from your domain unless the domain has been set up to prove which servers may send as it. That proof is what SPF, DKIM and DMARC do.

Part A. Stop others pretending to be you: SPF, DKIM and DMARC

Think of them as three checks the receiving mail server can make on a message that claims to come from your domain:

- SPF is a public list of the servers allowed to send mail for your domain. For Microsoft 365 the record normally includes spf.protection.outlook.com and ends with -all, which tells receivers to reject mail from anywhere else. Microsoft recommends -all for Microsoft 365 domains.
- DKIM adds a digital signature to your outgoing mail so the receiver can tell it was not altered and really came from you.
- DMARC tells receivers what to do when a message fails SPF and DKIM: nothing (p=none), quarantine it (p=quarantine) or reject it (p=reject). Microsoft's goal for your custom domains is p=reject, reached gradually: start with p=none while you watch the reports, then move to quarantine, then reject.

A domain only needs one SPF record. SPF and DMARC records are created at your domain registrar or DNS host (often the same company), not in Microsoft 365. If you are not comfortable with DNS, ask the company that hosts your domain.

How to check this yourself

1. Sign in to the Microsoft 365 admin center and open the Domains page (under Settings). Select your domain, then select DNS records. This shows the records Microsoft expects for your domain, so you know where your domain's DNS is managed.
2. Check your SPF record. Use a free online DNS lookup tool (Microsoft suggests using such tools) and look up the TXT records for your domain. You are looking for one record that starts with v=spf1 and contains include:spf.protection.outlook.com. The end of the record should be -all. If there is more than one SPF record, or it ends with ~all, ask for help fixing it.
3. Check DKIM. In the Microsoft Defender portal (security.microsoft.com), go to Email and collaboration, then Policies and rules, then Threat policies, then Email authentication settings, and select the DKIM tab. For your own domain, the toggle should say Enabled. If it does not, select the domain: Microsoft shows two CNAME records to publish at your DNS host, and after they are published (it can take a few minutes or longer to be detected) you turn on the setting 'Sign messages for this domain with DKIM signatures'.
4. Check DMARC. Look up the TXT record for _dmarc.yourdomain.com with the same online tool. A record starting v=DMARC1 means one exists. Note what p= says. If there is no record, create one starting at p=none with a reporting address, as Microsoft's guidance describes, and watch the reports before tightening.

Note on onmicrosoft.com: if you only use the default yourname.onmicrosoft.com address, Microsoft already configures SPF for you and signs outbound mail with DKIM. Almost every real business uses its own domain, so you will probably need the steps above.

Part B. Stop phishing aimed at your staff

All Microsoft 365 plans with cloud mailboxes include built-in protection: anti-malware, anti-spam and spoofing protection. A 'first contact' safety tip (a banner that warns when someone is getting mail from a sender they do not usually hear from) is available in every plan but is off in the default policy; the Standard preset below turns it on. Business Premium adds Microsoft Defender for Office 365 Plan 1, which includes Safe Links (checks web addresses in mail, Office files and Teams), Safe Attachments, and impersonation protection that looks for mail pretending to be a specific colleague or domain.

The simplest way to get Microsoft's recommended settings without tuning them yourself is to turn on a preset security policy.

1. In the Microsoft Defender portal, go to Email and collaboration, then Policies and rules, then Threat policies, then Preset security policies.
2. You will probably see Standard protection and Strict protection switched off. Standard is the sensible starting point for most offices.
3. Slide Standard protection to On, select Manage protection settings, and choose who it applies to (all recipients is the usual answer). Follow the wizard. On Business Premium it also asks about the Defender for Office 365 settings.
4. Check that Built-in protection is not excluding anyone you care about. Built-in protection gives basic Safe Attachments and Safe Links protection to people not covered by the other presets, on plans that include Defender for Office 365.

> **Free plans**
>
> On Business Basic or Standard you still get the built-in protection and can turn on the Standard preset for its Exchange Online Protection settings. Safe Links, Safe Attachments and impersonation protection need Defender for Office 365, which Microsoft documents as included in plans such as Business Premium. Microsoft also offers a 90-day trial of Defender for Office 365 Plan 2 in the Defender portal if you want to see it first.

Part C. The human part

- Teach one habit: if an email asks for money, new bank details or a password, confirm by phone using a number you already have, not the one in the email.
- Make reporting easy. Tell staff to report a suspicious message rather than delete it, and who to tell.
- If someone clicks and enters their password, treat the account as compromised. Microsoft's guide says the first step is to disable the account while you investigate (if you cannot, reset the password), then revoke active sessions, review registered MFA devices, and check for forwarding rules (Chapter 5).

Where PCA Security Check fits

PCA Security Check reads your domain's real SPF, DKIM and DMARC records and shows what they say. It does not check your anti-phishing policies or Safe Links settings; use the steps in Part B for those.

5. Find and block hidden mailbox forwarding

Why it matters

When an attacker gets into a mailbox, one of the first things they often do is set a rule that quietly copies your mail to an address they control. They can read invoices, wait for a payment, and send the fake 'new bank details' email at the right moment. Because the mailbox still works normally, nobody notices.

> **A familiar story (illustration)**
> Weeks after a password was stolen and reset, the owner of a small firm keeps seeing customers reply to emails she never sent. The password was changed, but a rule that forwards every message mentioning 'invoice' to an outside address was still there.

Microsoft describes two kinds of automatic forwarding to people outside your company: Inbox rules that users (or attackers who control the account) create, and mailbox forwarding (also called SMTP forwarding) that administrators set. Microsoft lists suspicious Inbox rules, and recently added external email forwarding, among the signs of a compromised account.

What good looks like

- Automatic forwarding to outside addresses is switched off by default for everyone, in the outbound spam policy.
- If anyone genuinely needs it, that is a deliberate exception for named people, not an open door.
- You look at the forwarding report now and then.

How to check this yourself

1. Open the Exchange admin center (admin.exchange.microsoft.com), expand Reports, then select Mail flow, and open the Auto forwarded messages report. It shows messages automatically forwarded to outside domains, who is forwarding, the type (Inbox rule, mail flow rule or SMTP forwarding) and where they go. By default it shows the last 7 days; change the date range if it looks empty. The summary page can query up to the last 90 days.
2. Look at the Forwarding users and Recipient domain charts. Any forwarder you do not recognize needs a conversation. Any outside domain you do not recognize is a red flag.
3. Check the setting that controls it. In the Microsoft Defender portal, go to Email and collaboration, then Policies and rules, then Threat policies, then Anti-spam. Open the Anti-spam outbound policy (Default), select Edit in the forwarding section, and look at Automatic forwarding rules.
4. Read the value. Microsoft recommends choosing On or Off explicitly instead of leaving the default 'Automatic - System-controlled'. Since 2021 that default means forwarding is off for new organizations and for existing ones that were not using forwarding, but for some existing organizations it can still behave as on.

If something is not right

- Set Automatic forwarding rules to Off - Forwarding is disabled. Microsoft notes this disables any Inbox rules or mailbox forwarding that redirect messages to external addresses. The sender gets a bounce message when forwarding is blocked, so tell staff.
- If a few people genuinely need it, Microsoft's suggested approach is to create a separate outbound spam policy that allows it only for those users.
- For a mailbox you think was taken over, follow Microsoft's compromised-account steps: reset the password, revoke sessions, review MFA devices, and review mail forwarders and all Inbox rules, including hidden ones. Microsoft's guide gives the commands for this.
- Admin forwarding on a single mailbox: in the Exchange admin center, go to Recipients, then Mailboxes, select the mailbox and look under Email forwarding.

> **Plan note**
> The outbound spam policy is part of the built-in protection in all Microsoft 365 plans with cloud mailboxes. Microsoft's forwarding report page states no plan restriction, but check that the report opens for you. No upgrade should be needed for this chapter.

Where PCA Security Check fits

Version 1 of PCA Security Check does not look at mailbox forwarding or the outbound spam policy. This chapter is a manual check for now.

6. Keep file sharing under control in SharePoint and OneDrive

Why it matters

Sharing a file by link is one of the best things about Microsoft 365, and one of the easiest ways to leak data. Links can be forwarded, can outlive the project, and, if you allow them, can work for anyone who has the address without signing in.

> **A familiar story (illustration)**
> Dana shares the payroll folder with the bookkeeper using an 'Anyone with the link' address, for convenience. A year later the bookkeeper's mailbox is compromised. The link in an old email still works for whoever finds it.

Microsoft notes that external sharing is turned on by default across SharePoint and OneDrive, so it is worth looking.

The four levels, in plain English

Setting (Microsoft's name)	What it means
Anyone	People can share by a link that works without signing in. Most open. Microsoft lets you require these links to expire, or give view-only permission.
New and existing guests	Outside people must sign in, or enter a one-time code to prove who they are, before they can open what you share.
Existing guests	Sharing only with outside people who are already in your directory.
Only people in your organization	No external sharing at all.

Rule of thumb for most small offices: choose New and existing guests. That lets you work with clients and suppliers, while making sure they prove who they are. Use Anyone only if you have a clear need, and then limit how long links last.

How to check this yourself

1. Open the SharePoint admin center (from the Microsoft 365 admin center, select Show all if you do not see it in the menu). Expand Policies and select Sharing.
2. Under External sharing, read the level for SharePoint and for OneDrive. Microsoft says OneDrive's setting can be more restrictive than SharePoint's, but not more permissive.
3. Select More external sharing settings. Look at: whether guest access expires automatically after a number of days, whether Anyone links must expire, and the default link type under File and folder links. Microsoft's options for the default link are Specific people, Only people in your organization, and Anyone with the link, and the last is only available when external sharing is set to Anyone. Prefer Specific people or Only people in your organization as the default.
4. Look at who your guests are. In the Microsoft 365 admin center, go to Users, then Guest users. Remove anyone who no longer needs access.
5. Check who is allowed to invite guests. In the Microsoft Entra admin center, go to Entra ID, then External Identities, then External collaboration settings. Under Guest invite settings, Microsoft's options range from anyone in the organization, down to only users in specific admin roles, down to no one. A tighter choice means fewer surprises. Under Guest user access, the most restrictive option limits guests to their own profile.

If something is not right

- Set the organization level to New and existing guests unless you need Anyone.
- If you keep Anyone, set links to expire (for example 30 days) and consider view-only.
- Set a guest expiration, so access is not forever by default.
- If you turn sharing down, Microsoft says guests usually lose access within about an hour. Tell the people you work with first.

> **A catch**
>
> Microsoft warns that if you turn external sharing off and later turn it on again, guests regain access. If you want certain guests to stay locked out, remove them or turn off sharing on those specific sites first.

Where PCA Security Check fits

PCA Security Check checks for 'Anyone with the link' sharing in SharePoint and OneDrive, who can invite guests, and what guests can see. It does not review individual sites or files.

7. Cover the device basics

Why it matters

Your Microsoft 365 account is only as safe as the laptops and phones that open it. A lost phone with company email and no screen lock is an open door.

> **A familiar story (illustration)**
> A salesperson leaves a laptop in a taxi. If the drive is encrypted and the sign-in is protected, it is an expensive nuisance. If it is not, it is a data breach.

The basics, in order

- Every laptop and desktop is encrypted. On Windows this is BitLocker (Pro, Enterprise and Education) or the simpler Device Encryption, which Microsoft says turns on automatically when a device is set up with a Microsoft or work or school account.
- Every device gets updates installed.
- Every phone and tablet that opens company email has a screen lock. Better still, company data is only reachable through managed or approved apps.
- You know which devices are connected, and can wipe a lost one.

What your plan gives you

- Business Basic and Business Standard: Basic Mobility and Security, a free mobile device management tool in Microsoft 365. It lets you manage iOS and Android devices, set access rules, view device details and wipe devices. Windows 10 and 11 PCs are listed too, but Microsoft says that on Business Basic and Standard a noncompliant Windows PC is not blocked from Microsoft 365 and users are not prompted to enroll it, so do not rely on it for laptops. Microsoft notes that Intune supports more device platforms, such as macOS and Linux.
- Business Premium: Microsoft Intune and Microsoft Defender for Business, which work with sign-in rules, so you can require a device to be marked as compliant before it can open company data.

How to check this yourself

1. Make a list of every device that opens company email or files: laptops, desktops, phones, tablets. Include personal phones.
2. On a Windows PC, open Settings, then Privacy and security, then Device encryption. If you see it, make sure it is On. If you do not see it, either your device does not support it or you are signed in with a standard account. On a Windows Pro PC you can use BitLocker Drive Encryption. A device that cannot be encrypted is a risk to note and plan to replace.
3. Open Settings, then Windows Update, and select Check for updates. If a device has not updated in months, fix that first.
4. On each phone, confirm a passcode or biometric lock is set and the operating system is current.
5. On Business Basic and Standard, Basic Mobility and Security is the free tool for managing phones and tablets (limited on Windows PCs). Setting it up takes several steps (Microsoft publishes a guide called 'Set up Basic Mobility and Security'), so ask your IT provider if you are not sure. On Business Premium, open the Microsoft Intune admin center (intune.microsoft.com) to see which devices are enrolled and which are marked compliant.

If something is not right

- Turn on Device Encryption or BitLocker on any unencrypted Windows device, and make sure the recovery key is saved to the account, not just the device.

- Set up a simple policy that requires a passcode on phones. On Business Premium, pair compliance policies with Conditional Access so that only compliant devices reach company data. Microsoft says that once Conditional Access and compliance work together, the result is an extra layer of security.
- Write a short 'lost device' routine: who to tell, who wipes it, and in what order (change password, revoke sessions, then wipe).

Where PCA Security Check fits

Version 1 of PCA Security Check does not look at devices. Use this chapter as a manual check for now.

8. Know what is backed up, and for how long

Why it matters

Many owners assume Microsoft keeps everything forever. Microsoft does keep deleted items for a while so you can recover from mistakes. But those windows are short, and they are recovery features, not a long-term backup you control.

> **A familiar story (illustration)**
> A former employee deletes a year of client folders on the way out. Nobody notices for five weeks. The recycle bin window has closed.

The windows you get without paying extra

What	What Microsoft documents	What it means
Deleted email	Items you permanently delete (for example by emptying Deleted Items) stay recoverable for 14 days by default. An admin can raise that to a maximum of 30 days. Calendar items are purged after 120 days.	After the window, a deleted message is gone for good
Deleted SharePoint files	Items are retained for 93 days from the time they are deleted from their original location, first in the site Recycle Bin, then, if that is emptied, in the site collection Recycle Bin for the rest of the 93 days (unless a site collection administrator empties it or it runs out of space)	About three months to notice and restore
OneDrive after a disaster	'Restore your OneDrive' lets you roll your whole OneDrive back to any time in the last 30 days (needs an active Microsoft 365 subscription). Files permanently deleted from the OneDrive recycle bin cannot be recovered this way.	Good against ransomware, if you act within 30 days
Audit log	Audit (Standard) is enabled by default and keeps records for 180 days	Lets you see who did what, for six months

If you need to keep things longer, or recover things that have been permanently deleted, you need a backup or a retention policy.

Your options

- Microsoft 365 Backup. Microsoft's own pay-as-you-go service for SharePoint sites, OneDrive accounts and Exchange mailboxes, with restore of whole sites, accounts and mailboxes. Microsoft's documentation lists the price as $0.15 per GB per month of data protected, billed on consumption rather than per user. Microsoft also offers directory (Entra) backup in public preview, priced separately. Check Microsoft's current pricing before you decide.
- A third-party backup service. Several companies sell backup built for Microsoft 365. Ask them what they cover (mail, OneDrive, SharePoint, Teams), how often, how long they keep it, and how a restore works.
- Retention policies in Microsoft Purview. These keep content for a set time even if users delete it. Availability depends on your plan, so check before you rely on it.

How to check this yourself

1. Write down what you would hate to lose: client files, accounting data, email archives, shared mailboxes.
2. For each, ask: where does it live in Microsoft 365, who could delete it, and how would I know?
3. Check the deleted item retention for mailboxes. Microsoft's default is 14 days. Ask your admin or reseller if it has been extended to the 30-day maximum.
4. Check whether any backup or retention setup exists. If someone says 'we have a backup', ask what it protects, how long it keeps copies, and when it was last restored as a test.
5. Do a small test. Delete a test file in OneDrive and restore it from the recycle bin, so you know the steps before you need them.

If something is not right

- Raise mailbox deleted-item retention to 30 days, the maximum. This is done in Exchange Online PowerShell (Set-Mailbox with -RetainDeletedItemsFor 30), applies to existing mailboxes only, and your IT provider can do it.
- Decide on a backup option and put a calendar reminder to test a restore each quarter.
- Tell staff that the recycle bin is not a backup, and not to rely on it.

Where PCA Security Check fits

PCA Security Check does not check backups or retention. This is a decision for you, with a vendor or your IT provider.

9. A 20-minute check to do every month

Security is not a one-time project. People join, people leave, and settings drift. A short, regular check catches problems early. Put it in your calendar for the same day each month.

The monthly routine

1. Admins (3 minutes). In the Microsoft 365 admin center, open Roles, then Role assignments, and look at Global Administrator. Any new or unfamiliar names? Anyone who has left?
2. Starters and leavers (3 minutes). Under Users, then Active users: are all accounts current employees? Did you block sign-in and remove licenses for leavers?

3. MFA (3 minutes). Confirm security defaults is still on, or that your Conditional Access MFA policies are still On. With Entra ID P1, open Authentication methods, then Activity, and look at how many users are capable of MFA.
4. Forwarding (2 minutes). Open the Auto forwarded messages report in the Exchange admin center (Reports, Mail flow). Anything new?
5. Guests (2 minutes). Users, then Guest users: remove anyone you no longer work with.
6. Secure Score (3 minutes). Open Microsoft Secure Score in the Microsoft Defender portal. Microsoft describes it as a measure of your security posture: a higher number means more recommended actions taken. Note the number, look at the top recommendations, and pick one to do this month.
7. Emergency access (1 minute). Do you know where the break-glass credentials are? Every 90 days, test them.
8. Updates (3 minutes). Ask whether every device has installed its updates. If you use device management, look at the device list.

> **About Secure Score**
>
> Microsoft gives every recommended action up to 10 points. If you cannot or do not want to do a recommended action, Microsoft lets you accept the risk. Do not chase the number for its own sake. Use it to see what is left and to watch the trend.

Keep the notes you made in the earlier chapters. If something changes unexpectedly, you will know the old value and the date.

Where PCA Security Check fits

After your first report, PCA Security Check offers a monthly re-scan: the same read-only check every month and a new emailed report, $29 a month for up to 50 users ($49 a month for 51 to 300 users), cancel any time. It covers the checks listed in this guide's earlier notes, not the manual items in this routine.

The one-page checklist

Tick each box when you have checked it yourself and fixed it if needed. Date it. Next month, do the quick version in Chapter 9.

Sign-in

- ☐ Security defaults is on, or Conditional Access requires MFA for all users
- ☐ Administrators must complete MFA (ideally phishing-resistant)
- ☐ I can see who has registered a second sign-in method
- ☐ Legacy authentication is blocked, and I have asked about scanners and old apps

Administrators

- ☐ Fewer than five Global Administrators
- ☐ Everyone who has an admin role needs it and still works here
- ☐ Admins use a separate account for everyday email
- ☐ Two emergency access accounts exist, are stored safely and have been tested

Email

- ☐ SPF record is in place and ends with -all
- ☐ DKIM is enabled for my domain
- ☐ A DMARC record exists, and I know the plan to reach p=reject
- ☐ Standard preset security policy is on
- ☐ Automatic forwarding to outside addresses is Off in the outbound policy, and the forwarding report is clean

Files and guests

- ☐ External sharing is set to the lowest level I need
- ☐ Anyone links are off, or they expire and are view-only
- ☐ Guest access expires, and old guests are removed

Devices and recovery

- ☐ Laptops are encrypted and updated
- ☐ Phones have a screen lock, and I know how to wipe a lost one
- ☐ I know what is backed up, for how long, and who can restore it
- ☐ I have tested one restore

Every month

- ☐ 20-minute check done (Chapter 9), date: _____

Want the checking done for you?

Everything in this guide can be checked by hand, and you now know how. If you would rather not click through a dozen admin pages, PCA Security Check checks the main settings in these areas for you, as listed below.

PCA Security Check	
What it is	An automated, read-only scan of your Microsoft 365 settings. It makes a plain-English PDF report with every finding, why it matters and the steps to fix it in Microsoft's own admin pages, plus your Microsoft Secure Score.
Price	$199 one time for up to 50 users, $299 for 51 to 300 users
How it works	You pay. An administrator signs in on Microsoft's own page and approves read-only access. The scan runs, and the report is emailed to the administrator who approved it.
What it checks	17 checks plus Secure Score: sign-in protection, MFA for administrators and everyone, old sign-in methods, the number of top-level administrators, outside app approvals, guest invitations, 'Anyone' sharing links, and SPF, DKIM and DMARC.
What it does not do	It changes nothing and does not read email or files. It is not a penetration test or a compliance certificate. It does not check mailbox forwarding, email threat-protection settings, devices, backups or emergency accounts, which are covered by the manual checks in this guide.

Learn more at pca-tech.com.

This guide gives general information and is not legal advice or a guarantee of security. Microsoft changes its products and menus often, so confirm steps against Microsoft's current documentation at learn.microsoft.com. Microsoft, Microsoft 365, Entra, Defender, Intune, SharePoint, OneDrive and Exchange are trademarks of the Microsoft group of companies. This guide is independent information from PCA Technology Inc.