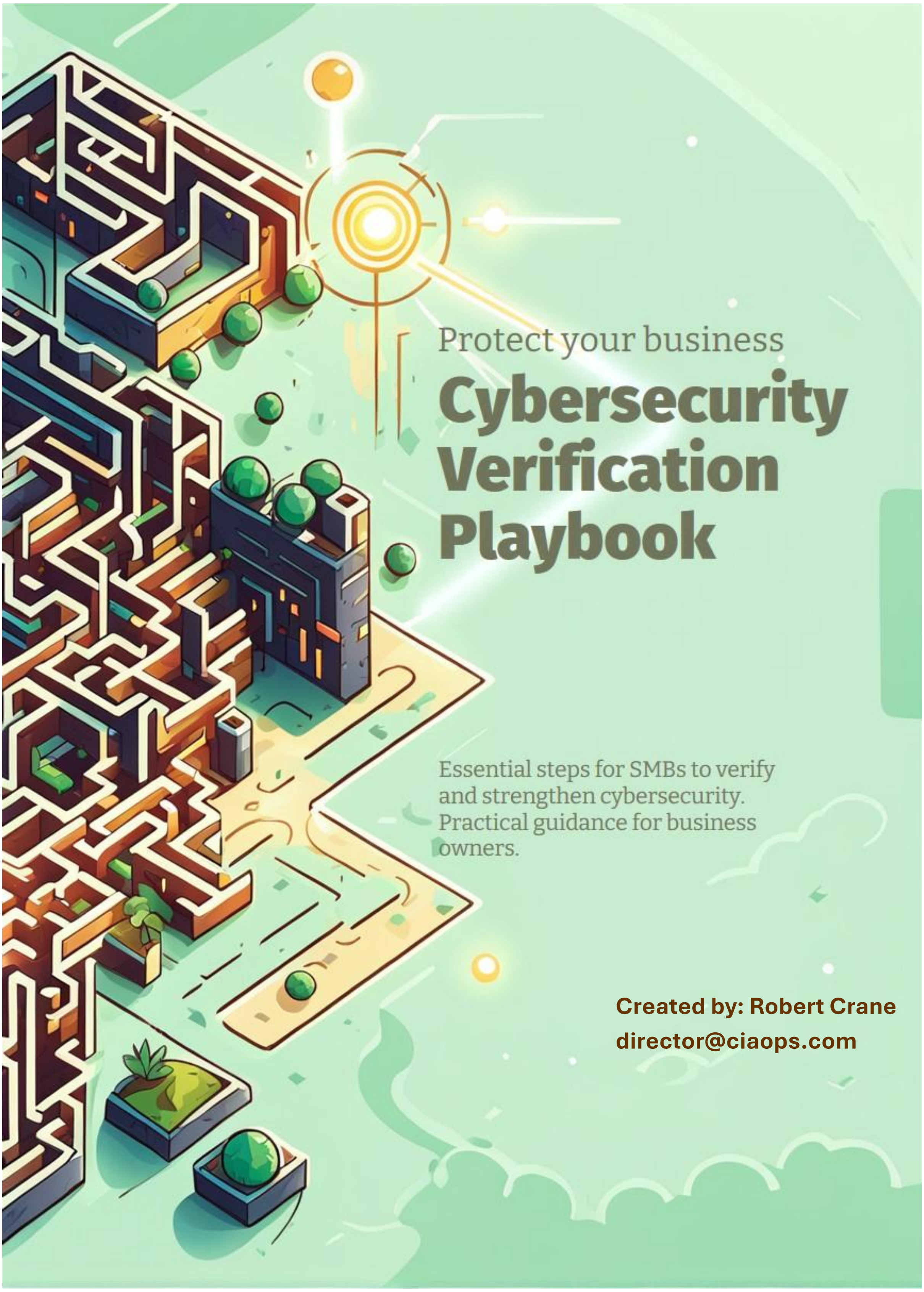


Protect your business

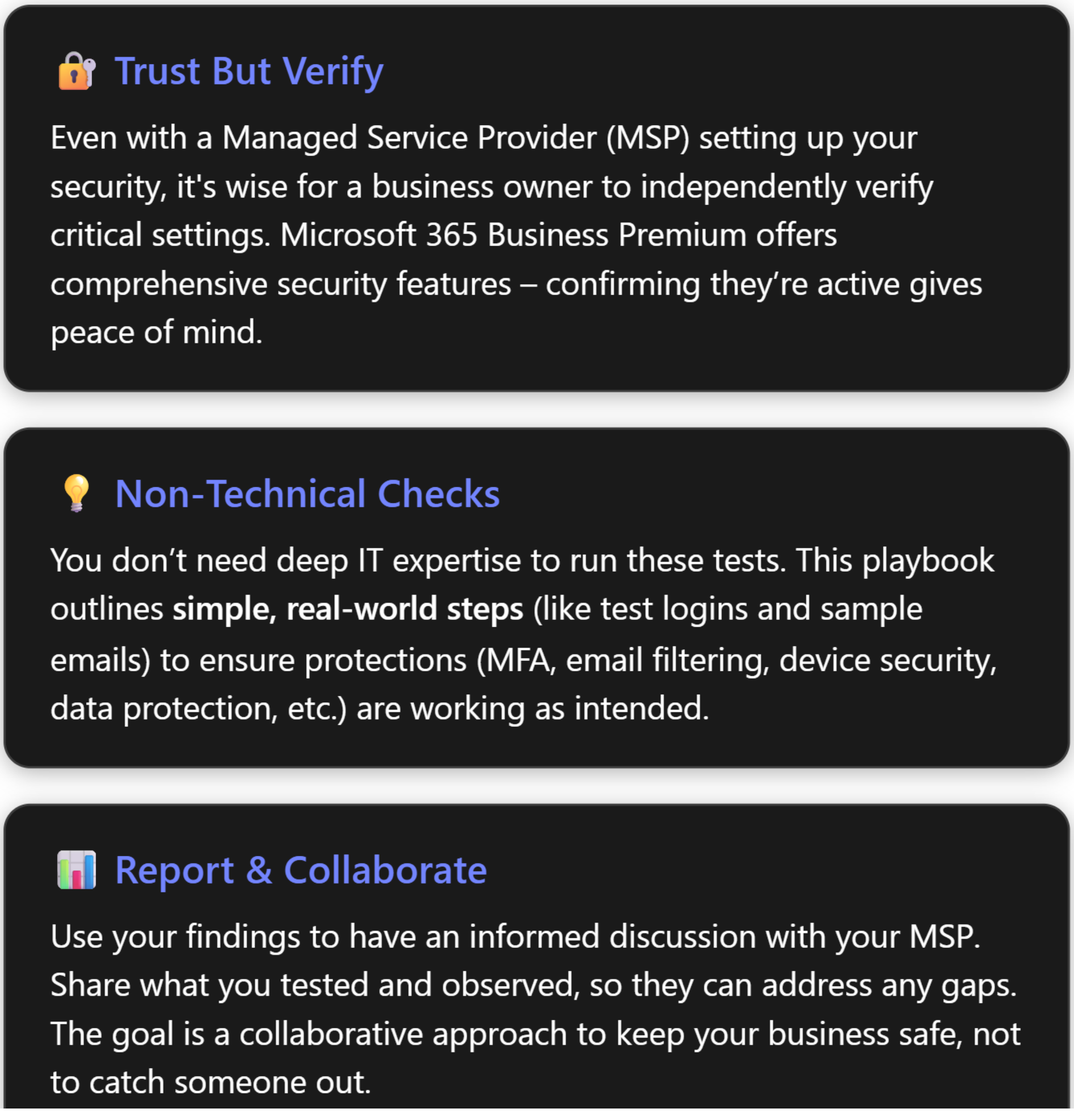
Cybersecurity Verification Playbook

Essential steps for SMBs to verify and strengthen cybersecurity. Practical guidance for business owners.

Created by: Robert Crane
director@ciaops.com

Microsoft 365 Business Premium Cybersecurity Verification Playbook

Ensuring your MSP-configured security is correctly in place and effective



🔐 Trust But Verify

Even with a Managed Service Provider (MSP) setting up your security, it's wise for a business owner to independently verify critical settings. Microsoft 365 Business Premium offers comprehensive security features – confirming they're active gives peace of mind.

💡 Non-Technical Checks

You don't need deep IT expertise to run these tests. This playbook outlines **simple, real-world steps** (like test logins and sample emails) to ensure protections (MFA, email filtering, device security, data protection, etc.) are working as intended.

📊 Report & Collaborate

Use your findings to have an informed discussion with your MSP. Share what you tested and observed, so they can address any gaps. The goal is a collaborative approach to keep your business safe, not to catch someone out.

Introduction

Microsoft 365 Business Premium is a **security-focused suite for small and medium businesses**, providing advanced protection for user accounts, emails, files, and devices [1] [2]. It includes features like multi-factor authentication for identity security, Microsoft Defender for Office 365 for email threat protection, Intune for device

[1] One simple action you can take to prevent 99.9 percent of attacks on your accounts

[2] Microsoft 365 for business security best practices - Microsoft 365 Business Premium | Microsoft Learn

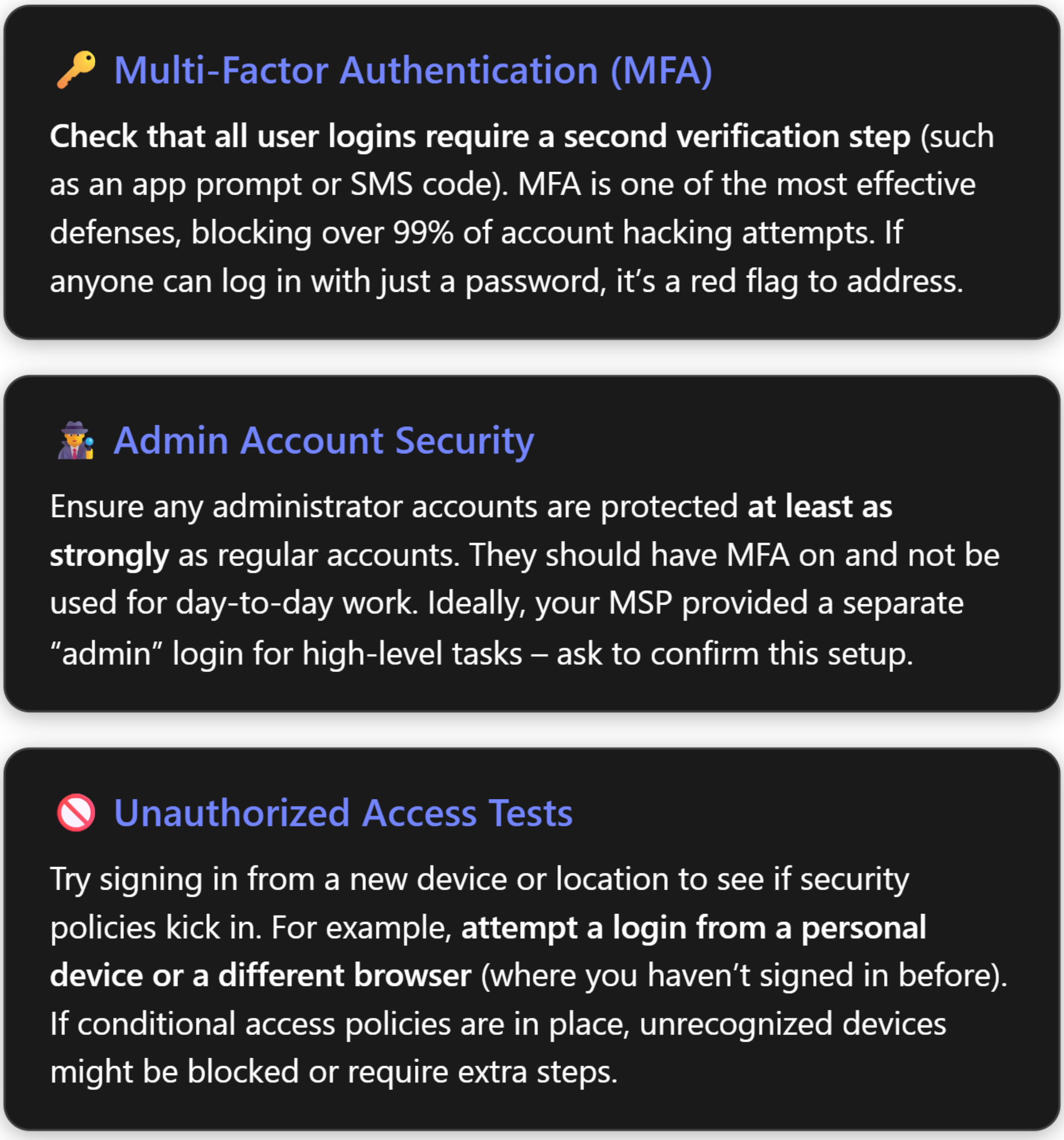
management, and Purview for data loss prevention (DLP) and information protection [1]. Your Managed Service Provider (MSP) likely configured these defenses – however, **mistakes or oversights can happen**. As a business owner, **verifying these configurations** is a smart way to ensure your organization is truly secure.

Why verify? Cybersecurity is ultimately your business's responsibility. Simple checks can confirm that critical safeguards (like MFA or backup policies) are actually enabled and working. This not only helps catch any misconfiguration early but also empowers you with a better understanding of your security posture. **Think of it as a due diligence audit** – you trust your MSP, but you also verify the essentials. Moreover, demonstrating vigilance in security can be important for compliance and insurance purposes.

This playbook presents a step-by-step approach to test and verify the key cybersecurity configurations in Microsoft 365 Business Premium, **using easy, non-technical methods**. Each section covers a major security area, with plain-language checks or exercises you can perform. We'll also cover how to interpret the results and *communicate them to your MSP constructively*. By following these steps, you can confidently answer whether your M365 Business Premium environment is configured correctly and securely.

Step 1: Verify Identity & Access Protections

The first layer of defense is controlling **who can access your systems and how**. M365 Business Premium includes strong identity and access management via Microsoft Entra ID (formerly Azure AD) [1]. Focus on verifying Multi-Factor Authentication and related sign-in security, since **compromised credentials are a top cause of breaches** [1].



🔑 Multi-Factor Authentication (MFA)

Check that all user logins require a second verification step (such as an app prompt or SMS code). MFA is one of the most effective defenses, blocking over 99% of account hacking attempts. If anyone can log in with just a password, it's a red flag to address.

🕵️ Admin Account Security

Ensure any administrator accounts are protected **at least as strongly** as regular accounts. They should have MFA on and not be used for day-to-day work. Ideally, your MSP provided a separate "admin" login for high-level tasks – ask to confirm this setup.

🚫 Unauthorized Access Tests

Try signing in from a new device or location to see if security policies kick in. For example, **attempt a login from a personal device or a different browser** (where you haven't signed in before). If conditional access policies are in place, unrecognized devices might be blocked or require extra steps.

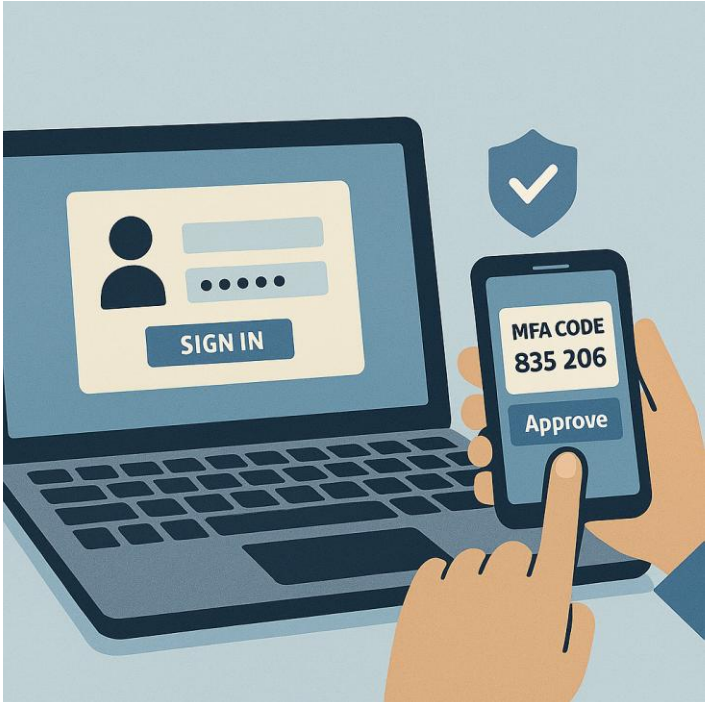
1.1 Ensure Multi-Factor Authentication (MFA) is enabled for all users: Microsoft 365 Business Premium supports MFA (also called two-step verification) by default, either via Security Defaults or custom policies [2]. To test this, **log out and log back into Microsoft 365** (e.g. portal.office.com) or use a private/incognito browser window. After entering your password, you **should be prompted for a second factor** (such as an authenticator app code or SMS code). If you can access your account with **only the password and no secondary challenge**, then MFA is not properly enforced for that account – flag this to your MSP immediately. Do this check for **each user or a sample of users** in your company (since sometimes an MSP might inadvertently leave one account without MFA). *Tip:* Also verify that **you and employees have set up your MFA methods** (Authenticator app, etc.) and know how to use them; lack of prompt could mean it's not set up or not required.

1.2 Check protection on administrator accounts: Administrator or global admin accounts have the **keys to the kingdom**, so they must be extra secure [2]. If your MSP uses a dedicated admin account (which they should), ask them to confirm those accounts also have MFA enabled and ideally use **phishing-resistant MFA** (like authenticator apps or FIDO2 keys, not just SMS). If you have any admin role on your tenant, perform the same re-login test for your admin account to ensure MFA triggers. Additionally, confirm with the MSP if they have an **emergency access admin account** (break-glass account) with MFA and strong password in case of lockouts – this is a best practice but that account should be used only in emergencies. As a non-technical check, *simply ask* your provider: *"Are all global/admin accounts secured with MFA and following least-privilege principles?"* They should be able to confidently say yes and explain any extra measures for admin security (like alerts on admin logins or using privileged identity management).

1.3 Test Conditional Access (if applicable): Many MSPs implement **Conditional Access policies** (available with Azure AD P1 in Business Premium) to add conditions on logins – for example, only allowing access from company-managed devices or requiring MFA when outside the office network. Without delving into Azure AD settings, you can **simulate an unauthorized login scenario** to see if the system correctly stops it. For instance, try logging into a company application (like Outlook Web or Teams) from a personal device that isn't set up by the MSP. If you have a home computer or a friend's device that isn't enrolled, try to sign in to your account. A properly configured policy **should block the access or ask for additional verification**. For example, a policy might say "block login from untrusted devices" – in that case you should **get an error or denial message** after entering credentials. No such block might indicate conditional access isn't configured or isn't working. *(Only perform this test for your own account and from a safe device!* If it doesn't get blocked, simply note that result and mention to the MSP – do not continue accessing sensitive data on an untrusted device.) Similarly, if your MSP set up **location-based restrictions** (e.g., only your country), you could use a VPN set to another country as a test – you should get blocked. These tests ensure the MSP's access rules (if in place) are effective. If you're unsure whether any conditional access policies exist, ask your MSP – if none, this step can be skipped but consider discussing if adding such policies is appropriate for your business.

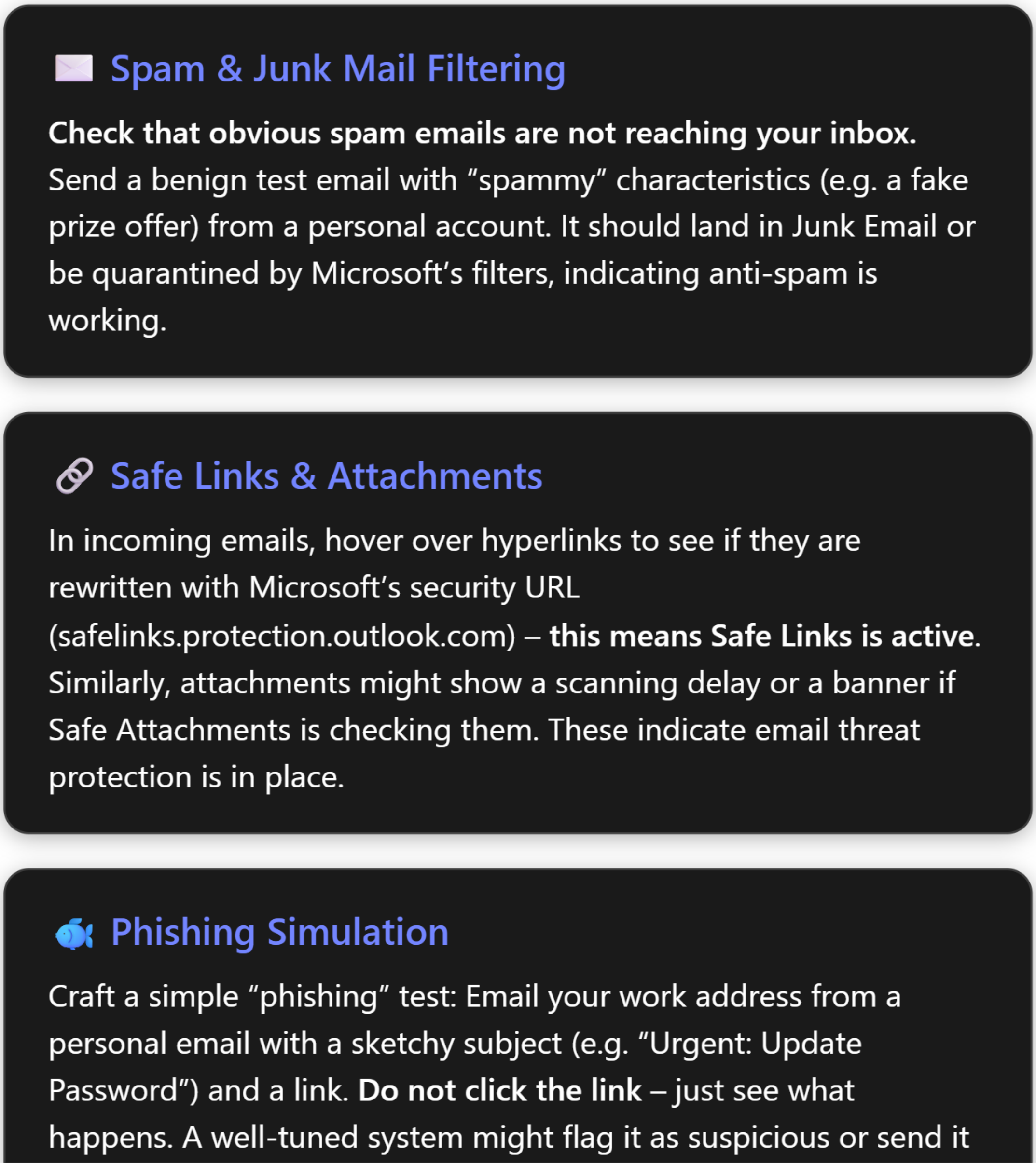
1.4 Review self-service options: As a minor check, see if **Self-Service Password Reset (SSPR)** is working (ask an employee to try the "Forgot my password" at login and see if they can go through MFA steps to reset – without actually changing it). Business Premium often enables SSPR so users aren't locked out; verify with MSP if this is set up. Also, ensure **legacy authentication is blocked** – this is hard to test directly as a non-admin, but you can ask if they disabled older protocols (to prevent attackers bypassing MFA via old email apps [1] [1]).

By the end of Step 1, you should have confirmed that **every account (especially admins) requires MFA**, and any advanced access policies are functioning. **Common issues to watch for:** MFA not enforced on a few accounts, default admin account left unprotected, or legacy login methods still allowed – these would need MSP attention.



Step 2: Test Email Security & Phishing Protection

Email is often the main entry point for cyber threats (phishing, malware, spam). M365 Business Premium includes **Microsoft Defender for Office 365** which provides anti-spam, anti-malware, and anti-phishing features on top of Exchange Online Protection [2]. Here you'll perform simple tests to ensure these email defenses are working:



✉️ Spam & Junk Mail Filtering

Check that obvious spam emails are not reaching your inbox. Send a benign test email with "spammy" characteristics (e.g. a fake prize offer) from a personal account. It should land in Junk Email or be quarantined by Microsoft's filters, indicating anti-spam is working.

🔗 Safe Links & Attachments

In incoming emails, hover over hyperlinks to see if they are rewritten with Microsoft's security URL (safelinks.protection.outlook.com) – **this means Safe Links is active**. Similarly, attachments might show a scanning delay or a banner if Safe Attachments is checking them. These indicate email threat protection is in place.

🐟 Phishing Simulation

Craft a simple "phishing" test: Email your work address from a personal email with a sketchy subject (e.g. "Urgent: Update Password") and a link. **Do not click the link** – just see what happens. A well-tuned system might flag it as suspicious or send it

2.1 Verify spam filtering and quarantine: One of the easiest checks is to ensure spam emails are being caught. If you have access to a **personal email account**, send a test message to your work email with some typical spam content (for example: a subject like "FREE $$$" and body with random gibberish or common spam phrases). Alternatively, copy a known spam email (remove any truly malicious links) and send it. **Expected result:** The email should **not land in your inbox**. It should either go to the "Junk Email" folder automatically, or be captured by the system quarantine. Microsoft

365's filtering should catch over 99% of mass spam. If your test email shows up directly in your Inbox with no warning, that's a concern (it might mean spam filtering settings are too lenient or misconfigured).

If your test went to Junk, great – the basics are working. You can also check the **Quarantine portal** for admins (or ask your MSP for a quarantine report). Often users get a **"quarantine summary" email from Microsoft** listing messages that were blocked [3]. If you or colleagues have received such quarantine notifications (for example, an email saying "2 messages are being held for you" [3]), that's evidence the system is actively catching potentially dangerous emails. Keep any quarantine notices as evidence of functioning email security.

2.2 Check Microsoft Defender for Office 365 features (Safe Links & Safe Attachments): Business Premium includes advanced email protection like Safe Links and Safe Attachments [2] (usually deployed via *preset security policies* set to standard or strict). **Safe Links** rewrites URLs in emails to protect you if you click a malicious link – you can spot this by hovering over a hyperlink in a recent email (especially from external senders). If you see a long URL starting with https://*safelinks.protection.outlook.com instead of the original domain, the Safe Links feature is **enabled and working** [2]. Try this on a known legitimate email that had links; you needn't click, just observe the hover tooltip.

For **Safe Attachments**, it's a bit less visible: when you receive an email with an attachment, sometimes there might be a small delay or a message like *"Scanning attachment..."* before you can download it. That indicates the attachment is being checked in a sandbox. You can test Safe Attachments by using the **EICAR test file** – a harmless file designed to trigger antivirus. *(If you're comfortable: download the "EICAR" test text file from eicar.org and attach it to an email from your personal account to your work account. The file is NOT a virus, but security systems treat it like one for testing.)* The email **should be blocked or the attachment stripped/quarantined** by Defender for Office 365. If the EICAR test email arrives in your inbox with the attachment accessible, then Safe Attachments or anti-malware might not be properly configured. **Note:** If you're not comfortable doing this, you can ask your MSP to run an antivirus test for you – they'll know the EICAR procedure. In any case, seeing any virus test or actual malware get through would be a serious issue to fix.

2.3 Test anti-phishing and impersonation safeguards: Phishing protection in Microsoft 365 includes detection of spoofed senders, impersonation of your domain or VIP users, and user reporting tools [2]. To do a simple phishing simulation: send an email from a **personal account** to your work address with something that looks phishy. For

[3] Sign in to Outlook

example, use a subject like “Important: Update Your Account Now” and in the body include text like “**Please login immediately .”> Make the sender name something odd or impersonating (you could even create a free Gmail in a name similar to your company). Do not click any test links** – the goal is to see how the system handles it. Possible outcomes: The email goes to Junk or Quarantine (ideal), or it comes to Inbox but with a warning banner like “This email is from outside your organization” (also a good sign that external tagging is on). Microsoft’s anti-phishing might also flag if the display name tried to impersonate one of your users or domains. If your test phish lands in the Inbox with no banner and looks just like a normal email, the phishing settings might be too weak. In that case, ask the MSP if anti-phishing policies (like domain impersonation protection) are enabled in Defender for Office 365.

Additionally, check if **users have a way to report phishing** easily: Look in Outlook (desktop or Outlook Web App) for a “Report Message” or “Report Phishing” button/add-in. Microsoft often provides this so users can click to report suspicious emails directly to Microsoft/your security team [4]. If it’s there, that’s a plus – try using it on the test phishing email you sent: did it successfully get removed or a confirmation shown? If the button isn’t there, consider asking MSP to deploy it (it’s part of Office 365 built-ins).

2.4 Outbound email safeguards: Sometimes misconfigurations allow outbound issues (like your account being used to spam others, or auto-forwarding corporate mail to personal addresses which can be risky). A non-technical check: Try setting an **auto-forward rule** in your mailbox to an external email (e.g., forward all mail to Gmail) and see if it works. Many security-conscious MSPs will **block automatic forwarding to external addresses** to prevent data leakage [5]. If your test forward is blocked or you get a warning, that means this protection is in place. If it forwards successfully, you might raise this as a concern – unless you require forwarding, it’s usually recommended to block it. Also, ask your MSP if **DKIM/SPF** email authentication is configured for your domain (you can use online tools to check SPF/DKIM records, or simply ask – they are important to prevent spoofing but not visible to end users).

After Step 2, you should have evidence that **email protections are operational**: spam is filtered, dangerous links/attachments are sanitized, and attempted phishes are caught or at least flagged. Document the results: e.g., “Test spam went to junk – ok”, “Test phishing got through without warning – not ok”. These observations will be shared

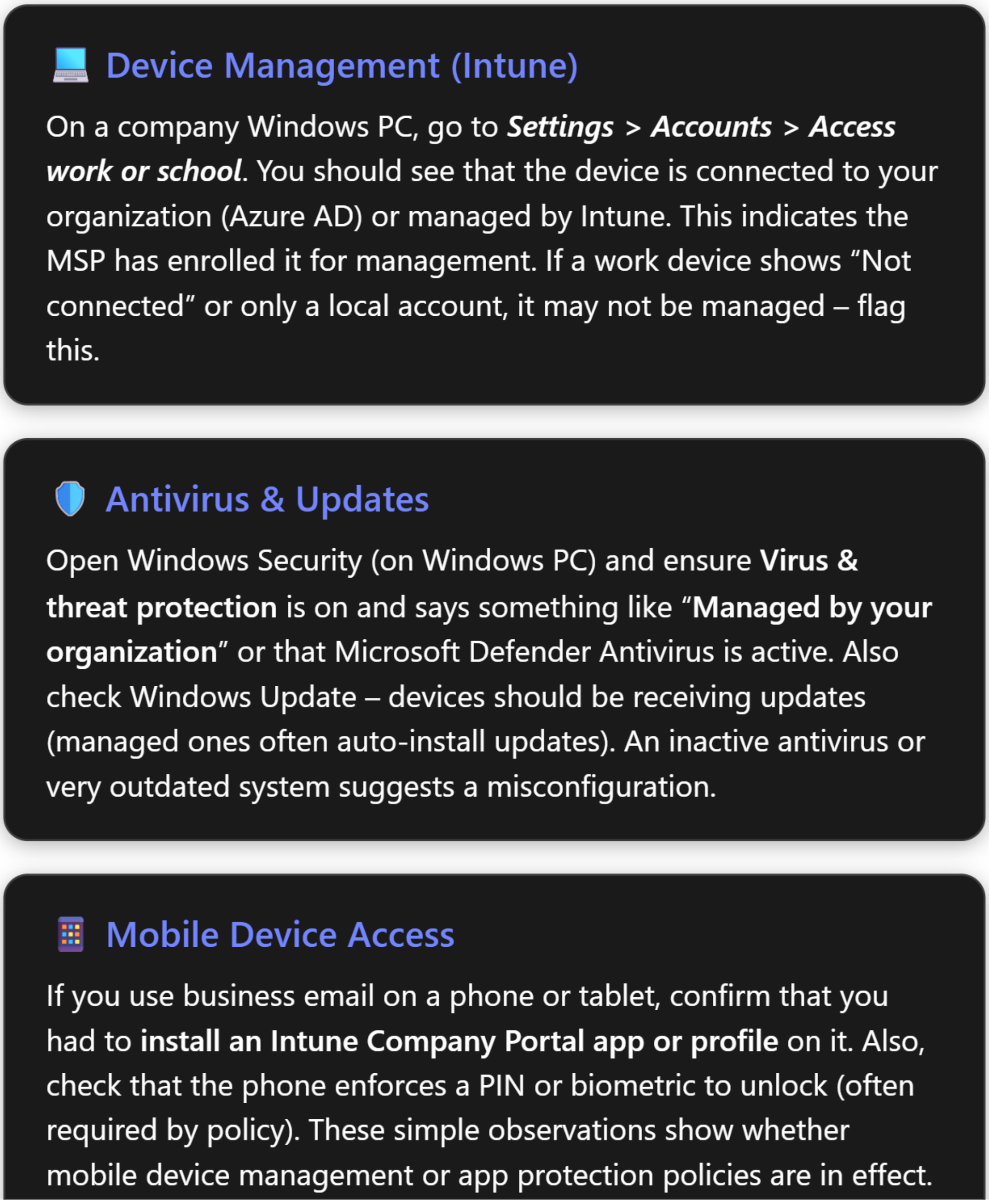
[4] Sign in to Outlook

[5] https://techcommunity.microsoft.com/t5/s/gxcuf89792/attachments/gxcuf89792/microsoft-365/47838/1/PracticalGuideToSecuringWorkFromAnywhereUsingMicrosoft365BusinessPremium.pdf

with the MSP. **Common gaps to check:** Safe Links/Safe Attachments not enabled (links aren't rewritten), no external email warning banner, or users not aware of how to report a phish. Each of these can be tightened up by adjusting the security policy – make note of anything off and continue.

Step 3: Check Device and Endpoint Security

Your computers, phones, and tablets (endpoints) need to be properly managed and protected, especially if they handle business data. Microsoft 365 Business Premium comes with **Microsoft Intune** (for device management) and **Microsoft Defender for Business** (for endpoint protection) [1]. This step ensures that your devices have the intended security policies from these services. Even a non-technical person can verify signs of device management and antivirus activity.



💻 Device Management (Intune)

On a company Windows PC, go to ***Settings > Accounts > Access work or school***. You should see that the device is connected to your organization (Azure AD) or managed by Intune. This indicates the MSP has enrolled it for management. If a work device shows “Not connected” or only a local account, it may not be managed – flag this.

🛡️ Antivirus & Updates

Open Windows Security (on Windows PC) and ensure **Virus & threat protection** is on and says something like “**Managed by your organization**” or that Microsoft Defender Antivirus is active. Also check Windows Update – devices should be receiving updates (managed ones often auto-install updates). An inactive antivirus or very outdated system suggests a misconfiguration.

📱 Mobile Device Access

If you use business email on a phone or tablet, confirm that you had to **install an Intune Company Portal app or profile** on it. Also, check that the phone enforces a PIN or biometric to unlock (often required by policy). These simple observations show whether mobile device management or app protection policies are in effect.

3.1 Verify PCs are enrolled in Intune (endpoint management): On a Windows 10/11 work computer, a quick way to check management status is: **Open Settings > Accounts > Access work or school.** There, you should see your work/school account connected. Clicking on it might show info like “Connected to Azure AD” or “managed by ”. This means the device is indeed enrolled in your company’s Azure AD/Intune management. Another indicator: In Settings > **Privacy & Security**, you might see “*Your device is managed by your organization*” messages or certain settings grayed out (because an admin policy controls them). These are positive signs that the MSP’s device policies are applied.

If instead you find **no work account connection on a company device**, or it’s just a local account, the device might not be managed at all – which is a problem to raise. For a deeper check (if you have some IT help), you can launch **Task Manager > Services** and see if the “Device Management Enrollment Service” is running, but that’s optional. On a **Mac used for work**, look for an MDM profile in System Preferences or an installed Company Portal app indicating enrollment. **Every company-owned device should be enrolled**. If you have any new device that wasn’t set up by MSP, try enrolling it following Microsoft’s guide (or ask MSP for instructions) to see if the process works (lack of enrollment could be oversight).

3.2 Check Microsoft Defender Antivirus and threat protection status: M365 Business Premium includes **Defender for Business**, an enterprise-grade antivirus/endpoint detection system [1]. For Windows devices, this is integrated as Microsoft Defender AntiVirus. To verify it’s working: open the **Windows Security** app (you can search the Start menu for it). Look at **Virus & threat protection**. It should show green check-marks or “no current threats”, and importantly, **check if it says “Managed by your organization”** anywhere, or if certain settings are locked. This implies Intune or security baseline policies are controlling it (a good sign). Also, check when the last virus scan ran and that virus definitions are up to date. You can even initiate a **Quick Scan** to ensure it runs without error.

For a more active test, again the **EICAR test file** can be used: if you copy that file to the PC, Defender should immediately flag and quarantine it. If it does, you know real malware would likely be caught. If it doesn’t, there’s a serious issue to discuss (Defender might be off or another antivirus is interfering).

Also confirm **Firewall** is on (Windows Security > Firewall & network protection should show active firewall on your network). Managed devices might also enforce features like **BitLocker disk encryption**. You can check if your C: drive is encrypted by going to Control Panel > BitLocker Drive Encryption (or This PC > right-click C: > Manage BitLocker). For a modern managed setup, BitLocker should be ON (this protects data if a laptop is lost). If you find it off on a laptop, ask why – maybe not configured, or perhaps it’s a desktop where it’s less critical. This is more technical, but easy to observe ON/OFF.

3.3 Ensure software updates and device compliance: See if your system is getting updates properly. In **Windows Update**, check the status – managed devices often say "*Your organization manages updates*" or will have most updates auto-installed. If you see a lot of pending critical updates or an OS version that's way out of date, it could mean update policies aren't effective. A non-technical employee could simply note: "My Windows is version X, last updated 3 months ago" – and that would prompt MSP to investigate. On phones, ensure the OS is updated as well (Intune can enforce minimum versions).

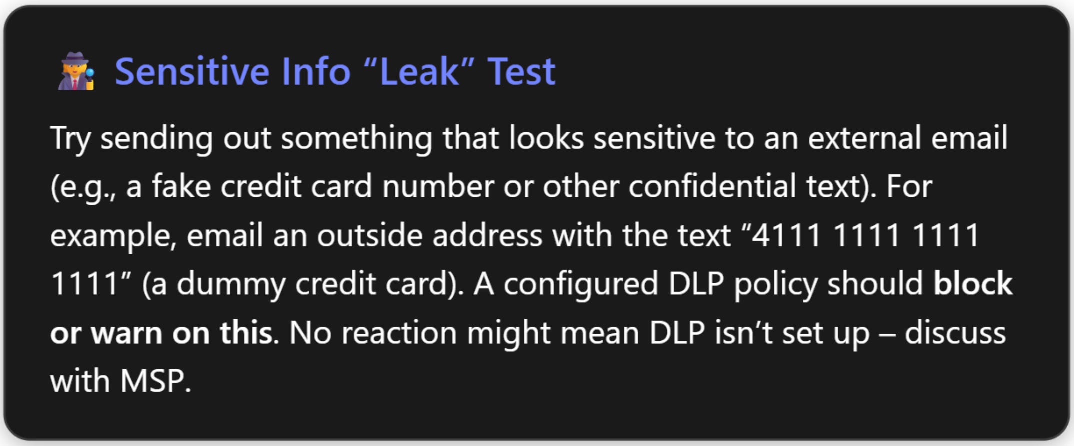
If your MSP has set up **Compliance policies** (to require certain security settings on devices), there's usually a compliance report. As a user, you might see notifications if your device is out of compliance (e.g., "You need to set a stronger password to access work resources"). No news is good news; it likely means your device meets all requirements.

3.4 Test access from an unmanaged device (for policy enforcement): This relates to Step 1's conditional access. If possible, try to open your work email or Teams on a completely personal device that was never enrolled. If Intune App Protection Policies (MAM-WE) are configured, you might still access email but with restrictions (like you can't copy text from Outlook to a personal app). It's hard to verify app protection as an end-user except by observing such restrictions. If nothing stops you from adding your work email to, say, the native mail app on your phone without any extra steps, then perhaps required app or device policies are not in place. Ideally, adding a work account on a mobile should prompt you to **install Microsoft's Company Portal** or at least enforce a device PIN and storage encryption on your phone. No prompt at all could indicate a lapse.

By completing Step 3, you confirm that **devices are under management and protected**: they're enrolled in Intune (or Azure AD joined), running Defender AV with up-to-date scans, firewalls and encryption are enabled, and they're receiving updates. **Common misconfigurations in this area:** devices not enrolled (MSP forgot to add a laptop), Intune policies not applied (devices showing compliance errors or no evidence of management), or Defender antivirus turned off due to a collision with another AV product. Bring these up with the MSP – they might need to push a policy or fix an enrollment issue.

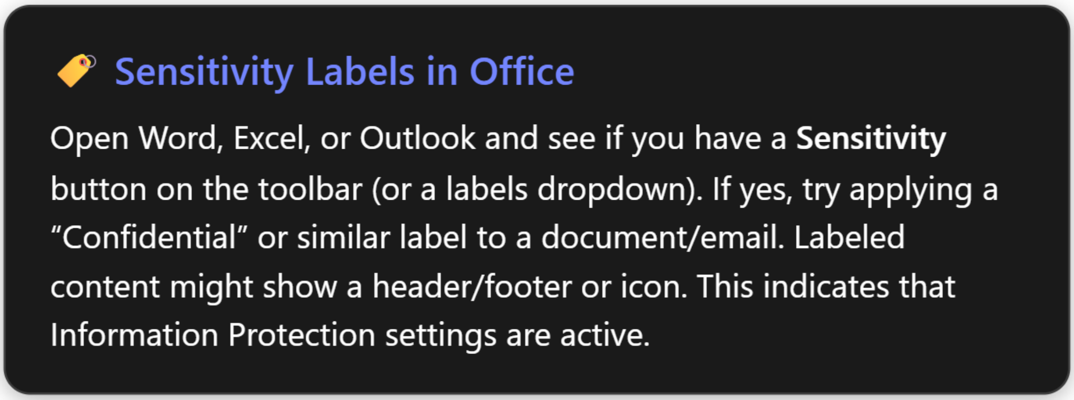
Step 4: Verify Data Protection (DLP, Sensitivity Labels, Backups)

Protecting your data – whether it's preventing leaks of sensitive info or securing files with proper labels/encryption – is another pillar of M365 Business Premium. Microsoft Purview features in Business Premium enable **Data Loss Prevention (DLP)**, **sensitivity labels**, and **message encryption** [1] [2]. In this step, you'll perform simple experiments to ensure that these protections are in place. The idea is to act as if you're accidentally trying to leak sensitive data, and see if the system reacts.



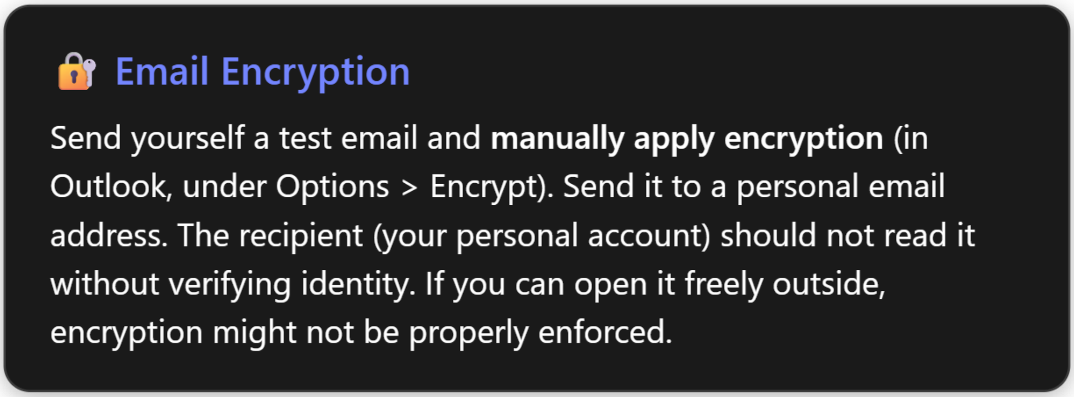
🕵️ Sensitive Info "Leak" Test

Try sending out something that looks sensitive to an external email (e.g., a fake credit card number or other confidential text). For example, email an outside address with the text "4111 1111 1111 1111" (a dummy credit card). A configured DLP policy should **block or warn on this**. No reaction might mean DLP isn't set up – discuss with MSP.



🏷️ Sensitivity Labels in Office

Open Word, Excel, or Outlook and see if you have a **Sensitivity** button on the toolbar (or a labels dropdown). If yes, try applying a "Confidential" or similar label to a document/email. Labeled content might show a header/footer or icon. This indicates that Information Protection settings are active.



🔐 Email Encryption

Send yourself a test email and **manually apply encryption** (in Outlook, under Options > Encrypt). Send it to a personal email address. The recipient (your personal account) should not read it without verifying identity. If you can open it freely outside, encryption might not be properly enforced.

4.1 Perform a Data Loss Prevention (DLP) policy test: M365 Business Premium often comes with a **default DLP policy** out-of-the-box to protect sensitive info like financial data or personal IDs [5]. To check if DLP is working, you can simulate sending sensitive data out of the organization: For example, create a new email in your work account to someone **outside** (your personal email works for this test). In the email, type a dummy **credit card number** such as 4111 1111 1111 1111 (this is a well-known test number used for demos – it's not a real card but looks like one). You can also add some text like "Confidential Project X data" in the body or subject. Send the email.

Expected results: If a DLP policy is in place and detects credit card numbers, one of a few things might happen:

- You might see a **policy tip** before sending, something like "This message contains sensitive information. Are you sure you want to send?" giving you a chance to override or cancel.
- The email might be **blocked** outright and you receive a notification (or a bounce message saying it violated policy).
- The email goes through, but you (the sender) or an admin gets a **alert notice** about it afterwards.

Any of these responses would indicate that DLP is active and catching the sensitive content. If the email sends with no warning and is received by the external account normally, **DLP may not be configured** (or the default policy might not cover that info type). Try a couple of variants if possible: e.g., sending a file containing personal data, or a message with the phrase "Top Secret" if you suspect they set up custom keyword-based rules. Keep it ethical and test with your own external accounts or willing partners – don't actually leak real data of course.

If all your tests slide through with no feedback, **make a note to discuss DLP with the MSP**. Perhaps they need to customize or enable policies. You can specifically ask, "What DLP policies do we have, and can we test them?" and share that your dummy data wasn't flagged. They might need to tune the system.

4.2 Check for Sensitivity Labels and Information Protection: Microsoft Purview also allows classifying and labeling documents/emails as Confidential, Public, etc., sometimes with encryption tied to those labels. Non-technical check: Open an Office application (Word, Excel, or PowerPoint) that's logged in with your work account. Look on the Home tab or the top menu for a button or dropdown that says **"Sensitivity"**. In Outlook, when composing an email, you might see an option to set a sensitivity label. If you see label options like *Public, General, Confidential, Highly Confidential*, then your MSP has published sensitivity labels for you [2].

As a test, **apply a "Confidential" label** to a test document or email. In Word/Excel, clicking a label might add a header or footer text (e.g., "Confidential") to the file automatically – check if that appears, which confirms the label applied. Now, what do these labels do? Some labels might be purely visual (just marking the document), but others could enforce encryption or access restrictions. A simple test: after labeling a

Word file as confidential, **try to open that file on a different account** (if you can simulate that – e.g., email the labeled file to a personal email and open there). If the label had protection, the personal account **should be blocked from opening the file or required to request access**. If the file opens fine externally and there was supposed to be encryption, then perhaps the label policy isn't correctly applied. This is a bit advanced to test alone, so another approach: ask the MSP for an **overview of what each sensitivity label does** (they should tell you if any automatically encrypt or only act as tags). At minimum, seeing that the **sensitivity labels are available** in your Office apps is good – it means the MSP set up Information Protection. If you don't see any label options in Office apps, then either labels haven't been configured for users, or the license isn't applied – bring that up ("Should we have sensitivity labels to classify data?").

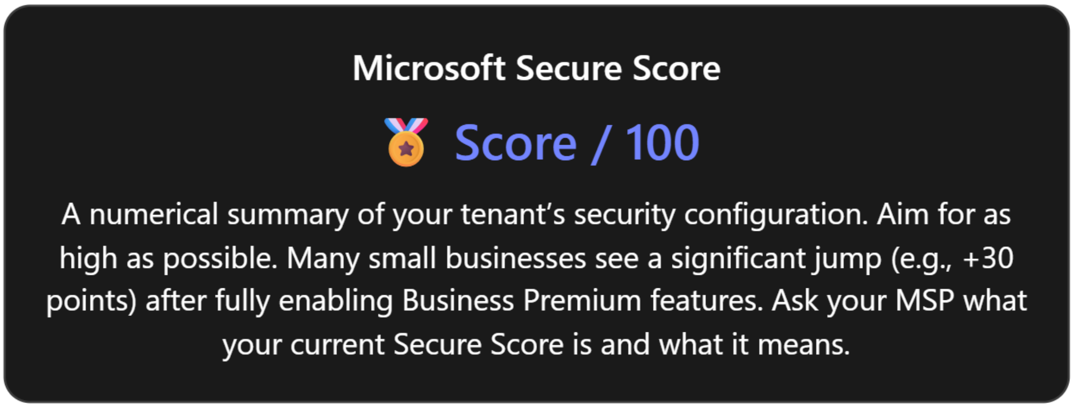
4.3 Test email encryption (Office Message Encryption): Even without labels, you can manually encrypt an email in Outlook using Office 365 Message Encryption, which Business Premium supports [1]. To do this, in Outlook desktop, create a new email to an external recipient. Before sending, go to **Options > Encrypt** and choose an option like "Encrypt-Only" or "Do Not Forward". Send the email. Then check at the external recipient side (for example, your personal Gmail). **Expected:** The external recipient should get a message indicating a protected email – usually they receive a link to view the message securely via a webpage, or if they also use Outlook.com, it might just show a small lock icon and enforce "Do not forward". The external user typically cannot read the content without signing in to a Microsoft account to decrypt, or using a one-time passcode to open it. This shows that encryption works. If instead the external mailbox receives the mail in plain text with no extra steps, something is off with the encryption configuration (or you might not have actually triggered the encryption properly – double-check your steps). This test is a bit technical, but it's a real-world scenario: say you need to send client data securely, you want to know that the "Encrypt" button actually does what it says.

4.4 SharePoint/OneDrive external sharing test: If your business uses SharePoint or OneDrive, you might want to test that **external sharing links respect security settings**. For instance, upload a dummy confidential document to OneDrive and try to share it with "Anyone with the link" if your policy allows. Many MSPs set sharing restrictions (like only allow sharing with specific domains or with password-protected links). If your attempt to create a completely public link is blocked or only "People in your organization" can be selected, that means the MSP has restricted sharing – which can be good. If you can generate an open, no-sign-in link freely, consider whether that's intended or a potential risk. (This depends on your business needs – open sharing might be needed, but it should be a conscious decision.)

By the end of Step 4, you should have tested that **data protection policies are effective**: your system noticed when you tried to send sensitive info out, and you have tools to label or encrypt data as needed. **Common issues:** No DLP policies catching anything, sensitivity labels not deployed, or users not aware of them, and lax sharing settings. Document what you tried and what happened (e.g., “Sent fake credit card – was allowed through” or “Confidential label present and working”). These findings direct the MSP on what to adjust (they might need to enable the default DLP or create custom rules based on your data sensitivity).

Step 5: Review Security Monitoring and Compliance Settings

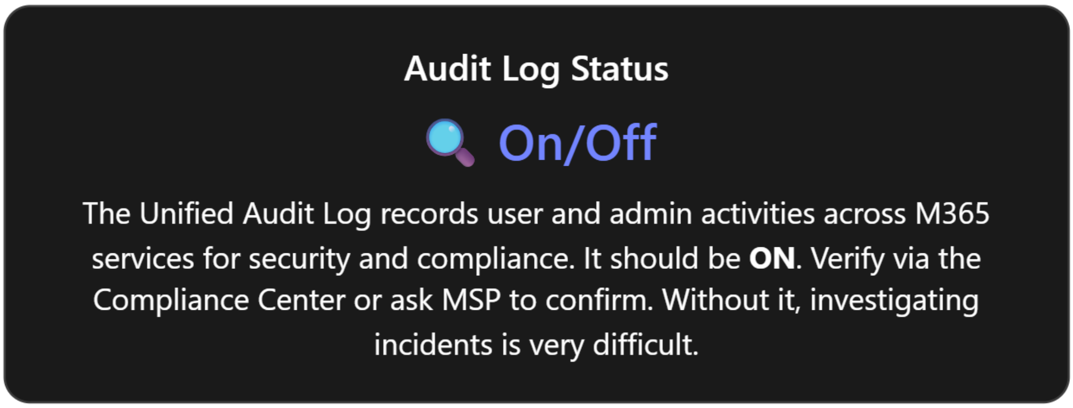
Beyond the front-line defenses, Microsoft 365 provides **monitoring and reports** to ensure everything is running securely. This includes things like Secure Score (a security posture rating), audit logs of user activities, and compliance configurations such as retention policies. In this step, you'll see what you can gather from available reports and ensure logging is in place. Even if you're not an expert, these tools often present info in a user-friendly way (or you can request reports from your MSP).



Microsoft Secure Score

🏅 Score / 100

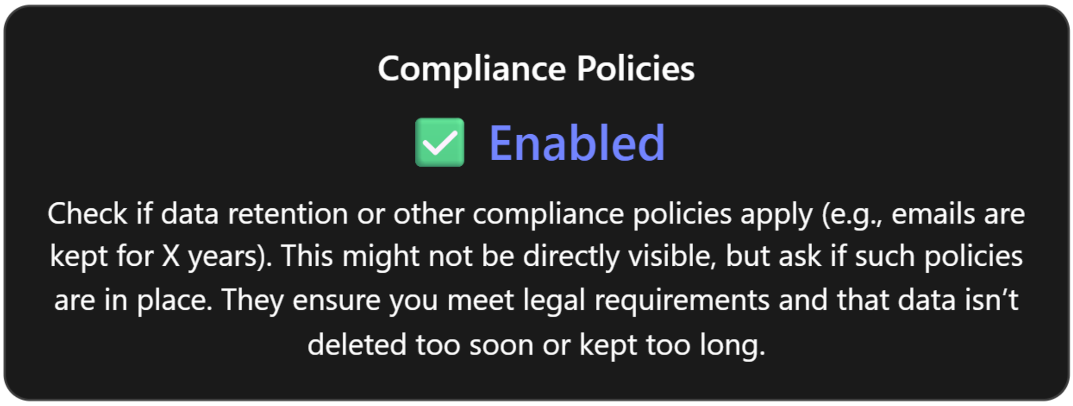
A numerical summary of your tenant's security configuration. Aim for as high as possible. Many small businesses see a significant jump (e.g., +30 points) after fully enabling Business Premium features. Ask your MSP what your current Secure Score is and what it means.



Audit Log Status

🔍 On/Off

The Unified Audit Log records user and admin activities across M365 services for security and compliance. It should be **ON**. Verify via the Compliance Center or ask MSP to confirm. Without it, investigating incidents is very difficult.



Compliance Policies

✅ Enabled

Check if data retention or other compliance policies apply (e.g., emails are kept for X years). This might not be directly visible, but ask if such policies are in place. They ensure you meet legal requirements and that data isn't deleted too soon or kept too long.

5.1 Check your Microsoft Secure Score: Secure Score is a Microsoft 365 dashboard that gives you a **score out of 100 (or more, depending on points) for your security configuration**, and lists improvement actions. If you have **Global Admin** or at least **Reports Reader** roles, you can access it yourself: go to the and look for Secure Score.

For a non-technical quick check, you might simply **ask your MSP to provide the Secure Score** for your tenant, along with any major recommendations it highlights. For example, if your Secure Score is, say, 45/100, that indicates many best practices are not yet implemented; a score of 70+ is better (few get 100 because some actions might not be applicable). Many organizations have improved their score significantly after configuring Business Premium security features [1]. It's a good quantitative measure to discuss. If possible, **review the Secure Score overview with your MSP**: it will show categories (Identity, Devices, Apps, Data, etc.) with points achieved vs. available. This can validate the results of Steps 1–4. For instance, if MFA wasn't enforced, Secure Score would flag that. If audit logging is off, that's flagged. Treat the Secure Score as a report card: it won't cover everything, but it's a great starting point for conversation.

5.2 Ensure Audit Logging is enabled: The Unified Audit Log is an essential logging mechanism in M365 that tracks user and admin activities (logins, file access, mailbox actions, etc.). By default, newer Microsoft 365 tenants have it **turned on**, but older ones might not. It's worth confirming because **without audit logs, investigating security incidents or suspicious behavior later is almost impossible** [6] [6]. If you have access to the Compliance Center as an admin (compliance.microsoft.com), you can check under **Audit**. If you see a big button saying "Start recording user and admin activities", that means it's OFF and needs to be clicked on [6]! If it's already on, you'll have a search interface for audit logs. As a quick test, you (or the MSP) could search the audit log for a recent activity, like "file accessed" or your test email from step 4, to verify events are being recorded [6].

For a non-admin, simply **ask your MSP: "Is our unified audit log enabled, and are we retaining logs for at least 90 days (or more)?**" The answer should be yes – Business Premium allows at least 90 days of log retention by default. If it was off and got turned on only now, note that it only starts recording from that point forward. Given its importance for compliance and security, this check is crucial.

5.3 Request security reports or alerts: Microsoft 365 often sends out various security summaries. For instance, if you have Azure AD Premium P1 (part of Business Premium), you might get **weekly risky sign-in or identity protection reports** via email [7]. Ask the MSP if they monitor those reports and if there have been any notable alerts (like repeated failed logins, unusual login locations, malware detections on devices, etc.). They might be using a SIEM (Security Information and Event Management) or dashboards in Defender portal. While this is their job, **as the client you have the right**

[6] How to Enable Unified Audit Log in M365 – Managed IT Services – IT support ,consulting, and service provider

[7] Sign in to Outlook

to be briefed regularly. You can establish a routine where the MSP delivers a monthly security report to you covering things like: number of blocked emails, devices out of compliance, any incidents handled, and Secure Score trend. If they aren't doing this, proposing it shows you are proactive.

If you do have admin access, also check **Alert Policies** in the compliance/security center – ensure there are policies configured for key events (e.g., malware detected, data loss incident, unusual mailbox forwarding). Microsoft often has default alerting for certain things. You might not validate this directly, but an MSP can show you "Yes, we have alerts set up – here's what would happen if X occurs."

5.4 Verify compliance configurations: Depending on your industry, certain compliance settings should be in place. A common one is **retention policies** – e.g., emails are kept for at least 7 years, or Teams chats for 1 year, etc., to meet regulatory needs or company policy. You can attempt a simple check: delete a test file or email and see if you (or admin) can still recover it beyond the typical recycle bin period because of retention. For example, if a retention is in place, even after deleting from "Deleted Items", an email might still be discoverable by admin eDiscovery for the retention duration. This is hard to test directly without admin tools, so likely you will **ask the MSP** about it: *"Do we have any retention or backup policies for our emails and files?"* A well-configured tenant might use M365 retention for compliance or at least have a backup service for O365. If they stutter on an answer, it might be something to consider adding.

Also inquire about **compliance score or Compliance Manager** (the counterpart to Secure Score for compliance). This might be overkill for a small biz, but it doesn't hurt to know if you have any major compliance gaps (like missing data privacy controls).

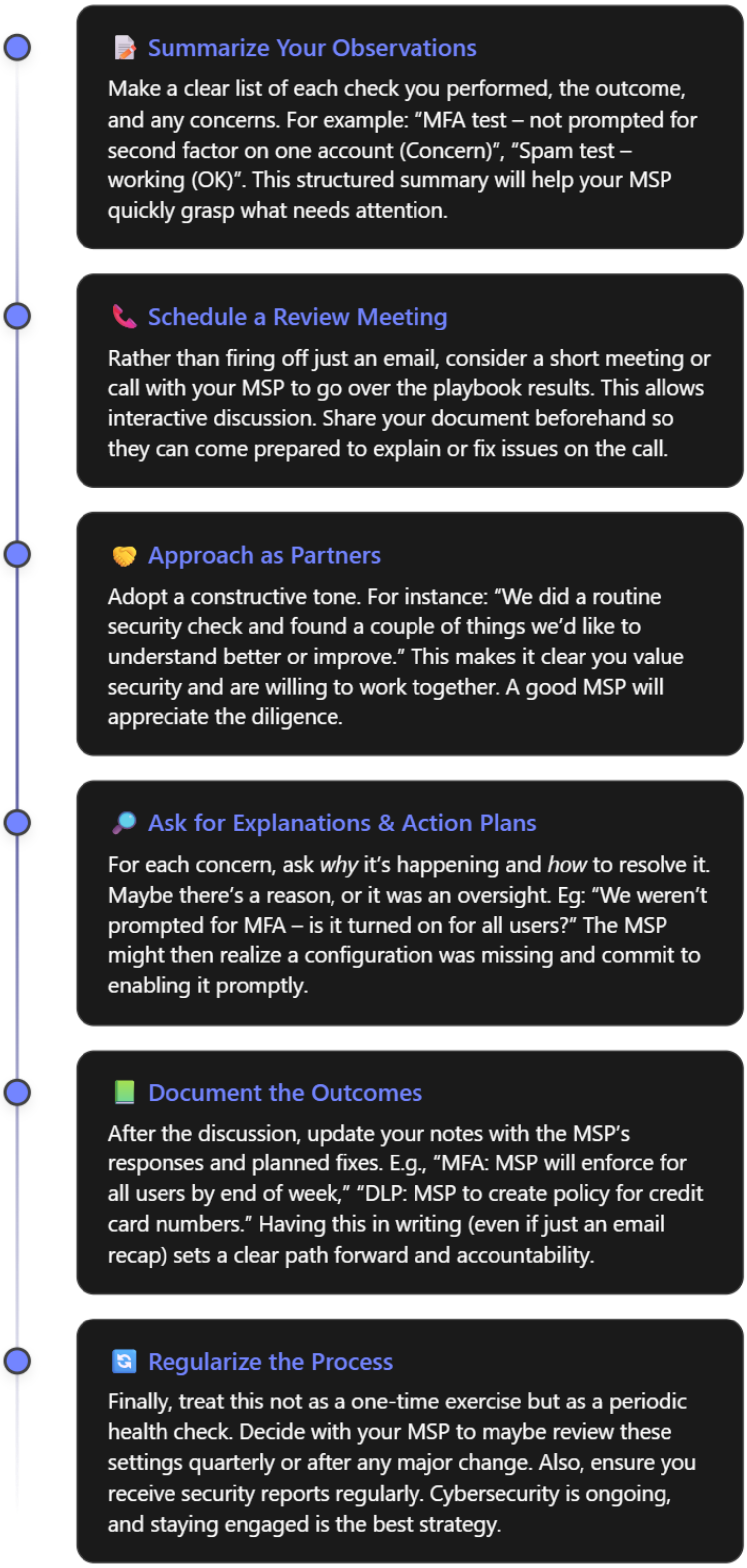
5.5 Confirm backup/recovery processes: While not strictly a configuration in M365 itself, ask how you would recover data if something happened. For example, "If we got hit by ransomware, do we have our SharePoint/OneDrive files versioned or backed up?" M365 has versioning that helps, but an MSP might add third-party backup. Since you're verifying security, include data resilience in the conversation. Non-technical verification here might be: restore a file from SharePoint's version history as a test (pick a document, make a change, then restore an earlier version to see if it works). Or try to recover a deleted email from the Recoverable Items (you can do this via Outlook by Recover Deleted Items). These tests confirm that *if* something were deleted or encrypted, you have the means to get it back.

By completing Step 5, you ensure that **the behind-the-scenes security governance is in order** – you have a sense of your overall security posture (Secure Score), your auditing and alerting is functioning, and compliance measures are addressed. It's less of a hands-on test and more of a review, but it ties everything together. **Common**

findings: Sometimes MSPs focus on frontline defenses but forget to enable audit logs or don't review Secure Score regularly. If your Secure Score is low or audit was off, don't be alarmed – use it as a roadmap for improvements.

Step 6: Report Findings and Discuss with Your MSP

Now that you've run through the playbook of checks and tests, it's time to compile what you learned and engage your MSP to address any issues. The relationship with your MSP should be a partnership – you're not "catching them" but rather collaborating to ensure nothing falls through the cracks. Here's how to effectively report and follow up:



📝 Summarize Your Observations

Make a clear list of each check you performed, the outcome, and any concerns. For example: "MFA test – not prompted for second factor on one account (Concern)", "Spam test – working (OK)". This structured summary will help your MSP quickly grasp what needs attention.

📞 Schedule a Review Meeting

Rather than firing off just an email, consider a short meeting or call with your MSP to go over the playbook results. This allows interactive discussion. Share your document beforehand so they can come prepared to explain or fix issues on the call.

🤝 Approach as Partners

Adopt a constructive tone. For instance: "We did a routine security check and found a couple of things we'd like to understand better or improve." This makes it clear you value security and are willing to work together. A good MSP will appreciate the diligence.

🔎 Ask for Explanations & Action Plans

For each concern, ask *why* it's happening and *how* to resolve it. Maybe there's a reason, or it was an oversight. Eg: "We weren't prompted for MFA – is it turned on for all users?" The MSP might then realize a configuration was missing and commit to enabling it promptly.

📗 Document the Outcomes

After the discussion, update your notes with the MSP's responses and planned fixes. E.g., "MFA: MSP will enforce for all users by end of week," "DLP: MSP to create policy for credit card numbers." Having this in writing (even if just an email recap) sets a clear path forward and accountability.

🔄 Regularize the Process

Finally, treat this not as a one-time exercise but as a periodic health check. Decide with your MSP to maybe review these settings quarterly or after any major change. Also, ensure you receive security reports regularly. Cybersecurity is ongoing, and staying engaged is the best strategy.

6.1 Prepare a clear report of your findings: Using the notes you took in each step above, compile a concise list of items to discuss. It's often helpful to categorize them as we did in this playbook (Identity, Email, Device, Data, Monitoring). For each category, list the tests and what you observed. Highlight any "Concern" or "Needs attention" items in red (or just with an asterisk and the word concern). For example:

- **Identity & MFA:**
  - MFA on admin – *Concern:* AdminAccount123 was able to login without MFA.
  - User MFA check – *OK:* All regular users prompted, except one user missing phone app (they used SMS).
  - Conditional Access – *Not sure:* was able to login from personal device, not blocked (need MSP input if that's expected).
- **Email Security:**
  - Spam filtering – *OK:* test spam went to junk.
  - Safe Links – *OK:* links are rewritten in emails.
  - Phishing test – *Concern:* clicked "Report Phish" but email remained in inbox (should it auto-remove?).
  - Auto-forward rule – *OK:* external forward was blocked (got admin notice).
- **Device Security:** ... and so on.

This level of detail shows you did your homework and helps the MSP pinpoint issues quickly. If some terms in your notes are too technical, don't worry – the MSP will understand them, or you can explain what you meant ("I sent a fake virus to test, it got through" is enough to convey the point).

6.2 Discuss in a constructive manner: When you meet or send the report, frame it as **proactive security maintenance**. You might say: *"We performed a security sanity-check using Microsoft's recommended best practices to ensure everything is correctly configured. Most things look good (mention those positives!), but we did find a few items we'd like your help to address or explain."* Acknowledge what **is** working well – e.g., if spam filtering and device management were solid, mention that and thank them. Then go through the concerns: ask if they were aware, and what the plan is. There might be quick fixes (enabling a setting) or they might educate you ("Actually, that test appeared to go through because of X, but here's why it's actually protected..."). Be open to their expertise too. The goal is to ensure both sides are on the same page regarding security.

For example, if MFA was off for one account, the MSP should say "Oops, we missed that, we will enforce MFA for that account right away." For something like DLP not catching your test, they might say "We haven't enabled DLP yet, but we agree it's important – we will configure a policy for that." In some cases, they might explain a weird result: e.g., "Your test phishing wasn't flagged because it came from your personal Gmail, which isn't on a threat intel list; however, real phishing from known bad domains would be flagged." If the explanation sounds unsatisfactory and leaves a real risk, don't hesitate to press for enabling the protective feature anyway.

6.3 Agree on remediation steps and timeline: For each identified gap, get a commitment on what will be done. It may help to prioritize: MFA issues are High priority (fix immediately), while maybe an issue like "no external email banner" is Medium (fix soon) and something like "BitLocker not on one old desktop" might be Low (schedule later but track it). Write these down. After the meeting or call, send an email **recapping the agreed actions** to the MSP, so there's a record. For instance: *"Thanks for reviewing the security checks with me. To recap, we agreed you will enable MFA for the admin account and ensure all users are covered by Friday. We'll also proceed to set up a basic DLP policy for credit card numbers this month. You will also look into why the phishing report button didn't remove the email and get back to me. Let's touch base in a month to see all these are in place and maybe run through the tests again."* – This kind of summary not only helps ensure follow-through but also signals that you're going to verify again. A responsible MSP will respect that.

6.4 Continual engagement: Security is not "set and forget." Threats evolve, and Microsoft releases new security features and recommendations regularly. Work with your MSP to schedule **periodic security audits** (perhaps annually by a third party, or quarterly internally) in addition to your informal tests. Also, stay informed: you as a business owner can subscribe to Microsoft's security blog or even brief newsletters (many MSPs send out updates) to know if there's something new you should ask your MSP about (e.g., "I heard there's a new ransomware protection setting – do we have that?"). Your active interest will ensure the MSP also stays on their toes. In fact, many MSP contracts have a clause about maintaining best practices – your verification helps ensure you're getting the service you're paying for.

Finally, foster a culture in your business that employees can speak up about security concerns too. If an employee finds they weren't asked for MFA or they got a strange email, they should feel comfortable telling IT or you – and then you can loop in the MSP. Involving everyone in basic security awareness (Business Premium includes training resources, and point #5 in Microsoft's recommended top 10 is training everyone on phishing [2]) complements the technical controls you've verified.

Conclusion

By following this playbook, you've taken a thorough tour of your Microsoft 365 Business Premium security setup from an end-user perspective. You identified key cybersecurity features – **from MFA and Conditional Access, to email threat protection, device management, DLP, and audit logging – and put them to the test**. None of the steps required deep technical skill, just a bit of curiosity and careful observation. This demonstrates that **even non-technical business owners can and should validate their cybersecurity posture.** After all, you have a lot at stake: your business data and operations rely on these defenses being sound.

Your findings, backed with real-world tests, provide a solid foundation for a conversation with your MSP. **Most MSPs will welcome an engaged client** and will address any gaps swiftly. You've essentially done a mini security audit – a proactive measure that can prevent bad surprises later. Remember to keep the dialogue positive and focused on improvement. The end result should be a stronger, verified security stance where you have confidence that *"yes, our MFA is on, our emails are filtered, our devices are secure, and our data is protected."*

Going forward, consider integrating these checks into your routine – perhaps semi-annually run through a few of them, or whenever there's a major change (like onboarding a bunch of new staff or devices). Cyber threats aren't static, and neither is Microsoft's platform (new security features may become available in your subscription). Staying in the loop with both your MSP and the Microsoft 365 roadmap will ensure you continue to leverage Business Premium's full security potential.

In summary, you've empowered yourself to **verify and trust** your cloud security. With both you and your MSP actively caring for the configurations, you significantly reduce the risk of misconfiguration-related breaches. Keep this playbook handy, update it with any company-specific tests you discover, and rest easier knowing you've got a handle on your cybersecurity. **Secure business is good business – and you've just taken strong steps to fortify yours**. [1] [2]