Microsoft 365 security best practices: 5 configurations to review

Missteps like weak MFA enforcement, legacy auth, and excess admin access can open the door to attackers. Here's how to fix them before they're exploited.

Microsoft 365 offers strong built-in security, but a missing or misconfigured security setting can leave your environment exposed. Here are five common Microsoft 365 security oversights that put organizations at risk and how to fix them. These apply across Microsoft 365 Enterprise, Business, and Education tenants.

1. MFA not enforced for all users

The problem: In 2024, Microsoft announced that it would begin to roll out mandatory MFA for some applications, including Azure and the Microsoft 365 admin center. Still, many Microsoft 365 tenants still don't require multi-factor authentication (MFA) for every user. By default, MFA isn't enforced unless Security Defaults or Conditional Access policies are in place. That means users may still be able to log in with just a password.

Why it's risky: Passwords alone aren't enough. They're vulnerable to phishing, credential stuffing, and password spray attacks. Microsoft reports that over 99.9% of compromised accounts had MFA disabled. If attackers get credentials, they can walk right in—especially if legacy protocols are enabled (more on that below).

How to fix it:

- **Use Conditional Access policies** to require MFA for all sign-ins. Avoid blanket exclusions and aim for complete coverage.
- **Enable Security Defaults** if you don't use Conditional Access. This enforces MFA and blocks legacy auth with one switch.
- **Go phishing-resistant** by favoring push notifications or FIDO2 keys over SMS.
- **Train your users** so they understand how MFA works and why it matters.

Bottom line: Enforcing MFA is the single most effective step you can take to secure Microsoft 365. It turns stolen passwords into dead ends.

2. Legacy authentication still allowed

The problem: Legacy authentication protocols like POP3, IMAP, and SMTP don't support modern MFA. While Microsoft is phasing them out, many tenants still have them enabled—sometimes by accident.

Why it's risky: Legacy protocols are a popular target for password spray attacks because they bypass MFA entirely. Even if MFA is enabled, a single exposed protocol can be used as a backdoor. Microsoft telemetry shows that many compromised sign-ins originate from legacy auth clients.

How to fix it:

- **Block legacy auth** using Conditional Access policies or Security Defaults.
- **Disable unused protocols** like POP, IMAP, and SMTP AUTH in Exchange Online.
- **Upgrade apps** that rely on legacy auth to versions that support OAuth.
- **Restrict exceptions** if legacy access is absolutely required—limit it to specific accounts and IPs.

Bottom line: Disabling legacy authentication ensures that every sign-in goes through modern auth, where MFA and Conditional Access policies can do their job.

3. Too many global admins

The problem: It's common for organizations to assign too many users the Global Administrator (GA) role in Microsoft 365. Sometimes, IT teams share a GA account, or staff keep admin privileges long after they're needed. Many also skip using dedicated admin accounts, performing privileged tasks from their everyday logins.

Why it's risky: Global Admins can change security settings, access user data, create accounts, and more. Given the high level of privilege, every GA account is a top-tier target for attackers. If just one is compromised, your entire tenant is at risk. Over-provisioned access also means a greater chance of accidental misconfiguration. Worse yet, using a GA account for "daily driving" activities like checking email, signing into enterprise applications, or browsing the internet increases the odds of phishing or malware exposure.

How to fix it:

- **Keep GA roles to a minimum**—ideally 2–4 users total. Assign more specific roles like Exchange Administrator or User Administrator where possible.
- **Use dedicated admin accounts** that are separate from day-to-day user logins. Lock them down with strong MFA and no email access.
- **Enable Privileged Identity Management (PIM)** with Microsoft Entra ID Governance. PIM makes admin access temporary and auditable.
- **Create emergency access accounts** for break-glass scenarios. These should be cloud-only, excluded from Conditional Access, and monitored closely.
- **Secure all admin accounts** with MFA—no exceptions. Consider using FIDO2 keys or biometric methods. Monitor sign-ins for unusual activity.

Bottom line: The fewer standing Global Admins you have, the fewer paths an attacker can exploit. Least privilege isn't just a best practice—it's a survival strategy.

4. Over-permissive sharing in SharePoint & OneDrive

The problem: By default, Microsoft 365 allows users to share files via anonymous links that don't require sign-in. The default link type is often set to "Anyone with the link," and Teams allows external guests by default, unless explicitly restricted. Without careful oversight, users can unintentionally expose sensitive content to the public.

Why it's risky: Anonymous links can be forwarded to anyone, and there's no audit trail of who accessed them. That makes it easy for sensitive data to leak outside the organization without detection. Over time, sprawling external shares and unmanaged guest access increase your risk surface. If OneDrive is allowed to sync to unmanaged devices, data can end up on personal machines with weak security—or remain there after an employee leaves.

How to fix it:

- **Disable anonymous links** by setting external sharing to "New and existing guests" or stricter.
- **Change the default link type** to "Specific people" so users have to specify recipients.
- **Review external sharing regularly** using built-in reports or PowerShell. Ask owners to revalidate links and guest access.
- **Limit who can share externally**—consider restricting it to specific teams or managers.
- **Control device access** using Conditional Access or SharePoint settings. Block downloads or enforce browser-only access on unmanaged devices.
- **Use Sensitivity Labels and DLP** to restrict sharing of confidential content—even if users try.

Bottom line: Collaboration doesn't have to mean open season on your data. Set sharing defaults that protect sensitive files and review them regularly. If you don't control external access, someone else will.

5. Inadequate email security configuration (SPF, DKIM, DMARC & phishing protection)

The problem: Email remains the most common entry point for phishing, malware, and business email compromise (BEC). While Microsoft 365 includes strong email security features, many organizations don't fully configure them. Common oversights include failing to set up **SPF, DKIM, and DMARC** email authentication protocols and leaving **anti-phishing and anti-spam policies** at their default settings in Exchange Online Protection (EOP) or Microsoft Defender for Office 365.

SPF is often set up during domain onboarding, but **DKIM and DMARC are frequently skipped**, leaving organizations exposed to spoofing and impersonation. At the same time, many tenants don't enable key anti-phishing features like **Safe Links, Safe Attachments, impersonation protection,** or disable risky features like **automatic external forwarding.**

Why it's risky: Without proper email authentication, attackers can **spoof your domain** in phishing campaigns—tricking customers, partners, or employees into handing over credentials or money. Weak anti-phishing policies mean **malicious emails are more likely to reach user inboxes,** increasing the risk of successful BEC scams.

If **auto-forwarding is enabled** or **malicious inbox rules go unmonitored,** attackers who compromise a mailbox can **quietly exfiltrate sensitive information** or hide critical emails, sometimes for weeks or months before detection.

How to fix it:

- Implement SPF, DKIM, and DMARC: Verify SPF is in place. Enable DKIM signing in the Exchange admin center for each domain. Publish a DMARC record in DNS—starting with

  ```
  p=none
  ```

  to monitor, then moving to

  ```
  quarantine
  ```

  or

  ```
  reject
  ```

  to block unauthorized senders.
- **Harden anti-phishing and anti-spam policies:** In Microsoft 365 Defender, configure protections for user/domain impersonation, enable Safe Links and Safe Attachments (if licensed), and tune spam/phishing thresholds beyond defaults.
- **Block external auto-forwarding:** Unless explicitly required, disable automatic forwarding to external recipients to prevent data leakage from compromised accounts.
- **Monitor mailbox rules and sign-ins:** Regularly audit inbox rules on high-risk accounts and enable mailbox auditing. Use sign-in risk detection (via Entra ID P2) to catch suspicious behavior.
- **Train your users:** Use simulated phishing tests and awareness campaigns to help employees spot and report malicious emails. Users remain a critical line of defense.

Bottom line: Misconfigured email security in Microsoft 365 leaves the door open to phishing, spoofing, and silent data theft. By enabling authentication protocols and tuning anti-phishing settings, you can block the most common attack vector before it reaches your users—and avoid becoming the next BEC headline.

How Nudge Security can help

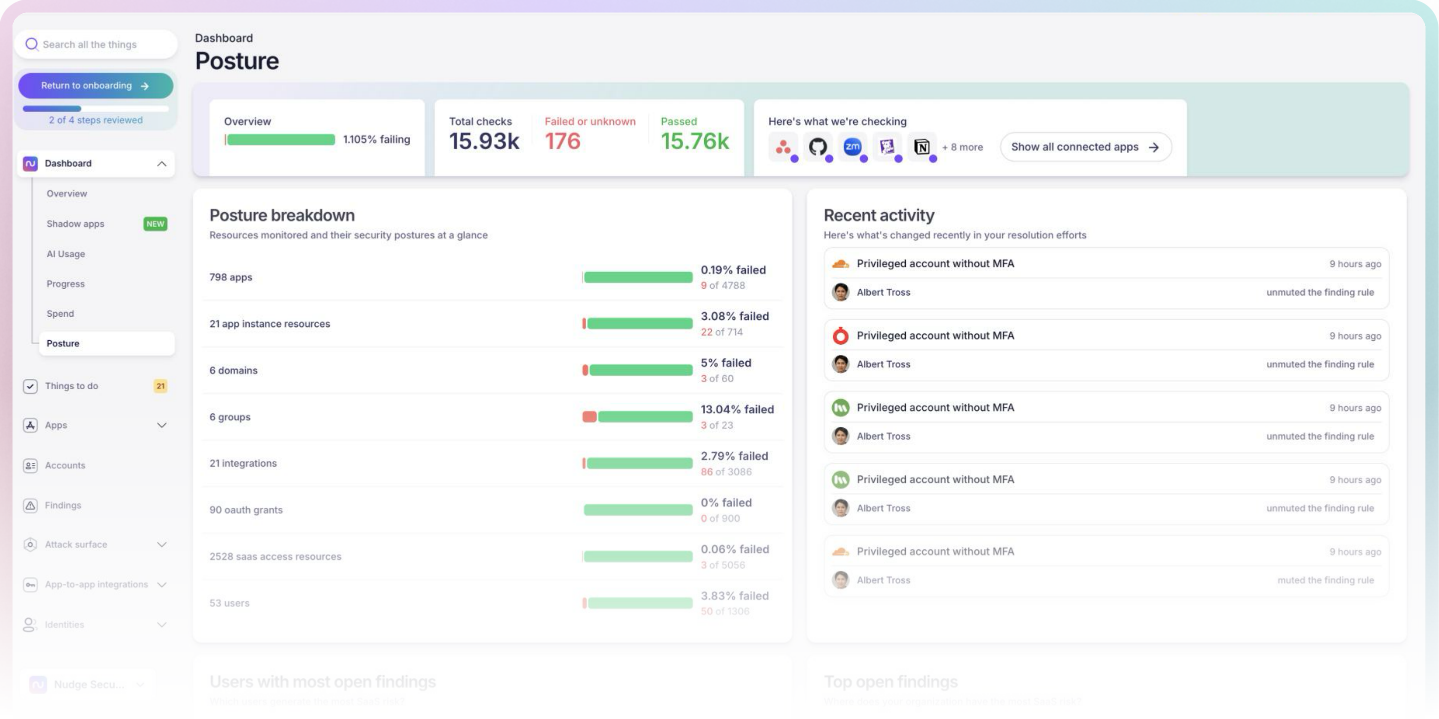
As this list shows, Microsoft 365 offers a wide range of powerful security features—but many of them require proactive configuration to be effective. Defaults aren't always secure, legacy settings can linger unnoticed, and it's easy to overlook risky gaps when managing a complex tenant. On top of that, Microsoft regularly adds new security controls, making it hard to keep pace without a systematic approach.

Nudge Security delivers security posture management for Microsoft 365 as part of a comprehensive SaaS security and governance solution.

With Nudge Security, you can continuously monitoring Microsoft 365 for misconfigurations, insecure defaults, and configuration drift to find risks like:

- Missing or misconfigured email authentication (SPF, DKIM, DMARC)
- Weak MFA enforcement and legacy authentication still enabled
- Excessive permissions granted to accounts or third-party apps
- Inactive accounts or mailboxes with lingering access
- Public sharing of Microsoft 365 resources like SharePoint sites or Teams files

Start a free 14-day trial now to see how Nudge Security can help you strengthen your Microsoft 365 security posture and proactively reduce risk across your entire SaaS environment.



Dashboard

Posture

Overview 1.105% failing

Total checks 15.93k | Failed or unknown 176 | Passed 15.76k

Here's what we're checking

Posture breakdown

Resources monitored and their security postures at a glance

798 apps	0.19% failed 9 of 4788
21 app instance resources	3.08% failed 22 of 714
6 domains	5% failed 3 of 60
6 groups	13.04% failed 3 of 23
21 integrations	2.79% failed 86 of 3086
90 oauth grants	0% failed 0 of 900
2528 saas access resources	0.06% failed 3 of 5056
53 users	3.83% failed 50 of 1306

Recent activity

Here's what's changed recently in your resolution efforts

Privileged account without MFA 9 hours ago
Albert Tross unmuted the finding rule

Privileged account without MFA 9 hours ago
Albert Tross unmuted the finding rule

Privileged account without MFA 9 hours ago
Albert Tross unmuted the finding rule

Privileged account without MFA 9 hours ago
Albert Tross unmuted the finding rule

Privileged account without MFA 9 hours ago
Albert Tross muted the finding rule

Users with most open findings

Which users generate the most SaaS risk?

Top open findings

Where does your organization have the most SaaS risk?