MICROSOFT 365 Security Quick Wins 2026

Ten high-impact actions every UK business should take this quarter.

Aligned with Microsoft, NCSC and Zero Trust principles

WHY YOUR TENANT IS THE TARGET

Microsoft 365 is the single most targeted business platform on the planet. It holds your email, your documents, your customer data, your financial records and for most UK businesses the keys to virtually everything else. That makes it both indispensable and a permanent target.

Over 80% of cyberattacks involve stolen or compromised credentials, and Microsoft 365 is the first door attackers try to breach. Phishing kits, password sprays, MFA fatigue attacks, token theft, business email compromise they all converge on the same goal: get into your tenant, monetise the access, and get out before anyone notices.

The good news is that most of the controls that defeat these attacks are already built into Microsoft 365. They simply need to be turned on, configured properly, and maintained. This guide covers the ten highest-impact actions you can take most of which can be implemented in hours, not weeks.

Use this guide as

- A 30-day hardening plan for your Microsoft 365 tenant.
- A working checklist for your IT team or managed service provider.
- A board-level briefing on where your business stands.
- A pre-incident audit far more useful than a post-incident one.

Who it's for

Business owners, IT managers and operations leaders running Microsoft 365 Business Standard, Business Premium or Enterprise tenants particularly those handling client data, working in regulated industries, or operating under ISO 27001, GDPR or Cyber Essentials.

Want a free Microsoft 365 security check?

Most tenants we audit have at least 3 of the 10 actions in this guide missing or misconfigured. We'll run a free security check against your tenant, identify the gaps, and give you a prioritised action list usually within five working days. No commitment, no obligation.

- Request your free M365 security check at systemforce.co.uk

1. ENFORCE MULTI-FACTOR AUTHENTICATION / PROPERLY

Multi-Factor Authentication is the highest-ROI security control your business can access. Microsoft's own data shows it blocks more than 99% of account compromise attacks. There is no other single setting that comes close. The catch: "enabled" is not the same as "enforced everywhere", and most tenants we audit have at least one gap.

Self-assessment

- MFA is enforced via Conditional Access not the legacy per-user MFA toggle, which is being deprecated.
- MFA is required for every user account, including admins, service desks, and shared mailboxes used interactively.
- Service accounts either cannot sign in interactively or are protected by a separate, monitored mechanism.
- Authenticator app or FIDO2 keys are preferred over SMS is vulnerable to SIM-swap attacks.
- Phishing-resistant MFA (FIDO2, certificate-based) is in place for all administrators.
- There is at least one break-glass account excluded from MFA, with strong, unique credentials and active monitoring.

What good looks like

Every successful sign-in to your tenant requires MFA, no exceptions. The policy is centralised, auditable, and consistent. SMS is being phased out in favour of authenticator apps and hardware keys, particularly for high-value accounts.

SFIT insight: We frequently see "MFA enabled" tenants that still have gaps, admin accounts on the legacy per-user toggle, or service accounts excluded "temporarily" three years ago. Conditional Access is the right way to enforce MFA in 2026, it's auditable, exception-aware, and gives you the policy framework for the next nine actions in this guide.

2. IMPLEMENT CONDITIONAL ACCESS POLICIES

Passwords plus MFA aren't enough on their own. Conditional Access evaluates the context of every sign-in who is signing in, from what device, from where, with what level of risk and decides whether to allow, challenge, or block. It's the engine that turns Microsoft 365 from a username-and-password system into a Zero Trust platform.

Self-assessment baseline policies

- Require MFA for all users, all applications.
- Block legacy authentication protocols entirely.
- Block sign-ins from countries you don't operate in (geofencing).
- Block sign-ins flagged as high-risk by Microsoft Entra ID Protection.
- Require compliant or hybrid-joined devices for administrative roles.
- Apply session controls (no download, sign-in frequency limits) for unmanaged devices.
- Maintain at least one break-glass account, excluded from CA policies, with strong credentials and alerting.

What good looks like

Identity decisions are based on signals, not just a valid password. Risky sign-ins are automatically blocked or challenged. Your users barely notice the security; attackers can't get past it.

SFIT insight: Conditional Access is powerful but easy to misconfigure and the failure modes are visible. We've taken on tenants who had CA deployed without testing, and it locked the entire business out for a morning. Always pilot first, always have a break-glass account, always document your policies.

3. DISABLE LEGACY AUTHENTICATION

Legacy authentication protocols, basic auth on Exchange, POP3, IMAP4, SMTP AUTH, entirely bypass Multi-Factor Authentication.

If they remain enabled in your tenant, your MFA strategy is theatre. An attacker with a valid username and password gets straight in, no second factor required.

Self-assessment

- Basic authentication is disabled tenant-wide in Exchange Online (Microsoft removed it for new tenants, but legacy tenants may still have residual settings).
- Legacy authentication is blocked via a Conditional Access policy.
- POP3 and IMAP4 are turned off per mailbox unless there is a documented business reason.
- SMTP AUTH is disabled tenant-wide and only enabled per-mailbox where required (and then monitored).
- Azure AD sign-in logs are reviewed for any remaining legacy auth attempts before fully disabling, to identify legitimate apps that need migration.

What good looks like

Zero successful sign-ins via legacy protocols in your audit logs. Any application or device that still requires legacy auth has either been migrated to OAuth, replaced, or is operating on a tightly scoped exception with monitoring.

SFIT insight: We always check the sign-in logs before turning off legacy auth. The classic surprise is a multifunction printer or a legacy line-of-business application using SMTP AUTH to send notifications turn off without checking, and you'll spend the next morning on the phone explaining why scanned documents aren't reaching anyone.

4. SECURE ADMINISTRATIVE ACCOUNTS

A compromised standard user is a problem. A compromised global administrator is a disaster full tenant access, the ability to turn off security controls, the ability to exfiltrate every mailbox, and the ability to hand the keys to anyone they want.

Admin accounts need a fundamentally different threat model from standard accounts.

Self-assessment

- Administrators have separate accounts for admin tasks, no day-to-day email, browsing or document work on admin identities.
- Admin accounts have no Exchange mailbox attached, removing email as an attack vector.
- Phishing-resistant MFA (FIDO2 keys ideal) is required for all administrators.
- Privileged Identity Management (PIM) is used to grant admin roles just-in-time, with approval and time limits.
- Admin role assignments are reviewed quarterly, with stale assignments removed.
- Admin accounts are named distinctly so they cannot be confused with standard users (e.g. adm-jbloggs).
- Sign-ins to admin accounts trigger alerts to a security mailbox or SOC.

What good looks like

Admin access is temporary by default, requires elevation, is logged in real-time, and is reviewed regularly. The number of standing global administrators fits comfortably in single digits.

SFIT insight: A surprising number of breaches we investigate involve a global admin account that hadn't been touched in months but still had full rights, often a former IT contractor, an outsourced project, or a "break-glass" account that had quietly become the main admin login. Quarterly admin reviews close this gap, and PIM (where licensing allows) handles the rest.

5. ENABLE MICROSOFT DEFENDER FOR OFFICE 365

Built-in Exchange Online Protection blocks bulk threats, spam, known malware, obvious phishing. Microsoft Defender for Office 365 (P1 included with Business Premium, P2 with E5) blocks the targeted ones phishing kits, malicious attachments, executive impersonation, business email compromise. If you have the licence, not turning it on is a missed open goal.

Self-assessment

- Preset security policies (Standard or Strict) are applied to all users.
- Safe Links is enabled, rewriting URLs in inbound email and Teams messages.
- Safe Attachments is enabled, sandboxing inbound attachments.
- Anti-phishing impersonation protection is configured for VIPs (directors, finance team) and your own domain.
- Users have a one-click "report phishing" button that sends to your IT or security team.
- Quarantined messages are reviewed regularly, and false positives are tuned out.

What good looks like

The threats that get past Defender are rare enough to investigate individually. External lookalike domains can't impersonate your finance team. End users have a clear, low-friction way to flag suspicious emails.

SFIT insight: We see Defender for O365 catching things that native Exchange Online Protection misses daily particularly executive impersonation and credential phishing. For Business Premium tenants, it's already in your licence; the only reason not to turn it on is that no one has.

Are you actually using the security tools you're paying for?
Most Business Premium and E5 tenants are licensed for far more security than they have configured. We can run a licensing-versus-deployment audit and show you exactly which tools you've already paid for but aren't using. It's usually a six-figure efficiency saving over the contract term.

- Book your licensing-versus-deployment audit at systemforce.co.uk

6. ENABLE UNIFIED AUDIT LOGGING

When something goes wrong, audit logs are the difference between "we know exactly what happened" and "we have no idea". They must be enabled before the incident, not after. By the time you suspect a compromise, it's too late to start logging.

Self-assessment

- Unified audit logging is enabled at the tenant level.
- Log retention is configured beyond the default, 90 days minimum, longer where regulatory requirements apply.
- High-risk events trigger alerts: new mailbox forwarding rules, mass file downloads, role assignment changes, suspicious sign-ins.
- Logs are exported to a SIEM or central log store where one is in use.
- There is a documented process for who reviews alerts, when, and what they do about them.

What good looks like

Your audit logs answer the questions an investigator would ask, who, what, when, from where, on what device, across the full retention window your business and regulators require. Alerts are actioned, not just generated.

SFIT insight: The single biggest red flag we look for in compromised tenants is a malicious mailbox-forwarding rule quietly siphoning copies of every email to an external address. Unified audit logging is what surfaces it, and yet we still find tenants with logging disabled "to save space". Don't be one of them.

7. IMPLEMENT DATA LOSS PREVENTION

Most data leaks aren't malicious someone forwards a spreadsheet to a personal email, shares a SharePoint folder with the wrong external user, or pastes a customer list into a private chat.

Data Loss Prevention catches these mistakes before they become incidents and gives you a fighting chance against malicious incidents, too.

Self-assessment

- DLP policies are in place for data covered by GDPR (UK NI numbers, financial records, health information).
- DLP policies cover Exchange, SharePoint, OneDrive and Teams.
- Sensitive industry data payment card numbers, HR records, contract data, has appropriate policies.
- Alerts are reviewed by a named person or team, with a documented response process.
- Policies have been tuned to reduce false positives that desensitise users.
- Users see clear, helpful policy tips when an action is blocked or warned, not generic error messages.

What good looks like

Sensitive data leaving your tenant raises an alert that someone actually responds to. Users understand why a particular share or send was blocked, and have a documented route to request an exception when there's a legitimate business need.

SFIT insight: DLP works best when it's tuned for your business generic templates flag everything and end up ignored. We typically run a discovery phase first to find out what sensitive data you actually have and where it lives, then build policies around that reality. The tuning matters more than the policy count.

8. ENFORCE DEVICE SECURITY WITH INTUNE

A perfectly secure tenant accessed by a compromised laptop is still compromised. Identity is one half of the access decision; device posture is the other.

Microsoft Intune lets you enforce that only managed, compliant devices can access company data and prove it during an audit.

Self-assessment

- All corporate Windows and macOS devices are enrolled in Intune.
- Compliance policies require disk encryption (BitLocker / FileVault), supported OS versions, and active endpoint protection.
- Conditional Access blocks Microsoft 365 access from non-compliant devices.
- Mobile devices are either fully managed (corporate-owned) or have App Protection Policies applied (BYOD).
- Lost or stolen device wipe procedures are documented and tested.
- There is a clear distinction between corporate and personal device profiles.

What good looks like

Only managed, compliant devices can access company data and you can demonstrate it from the Intune console at any time. Personal devices that access work data protect corporate data without intruding on the user's personal life.

SFIT insight: BYOD is where this gets tricky. App Protection Policies (without enrolling personal devices) are a strong middle ground they protect corporate data in the Outlook and Teams apps without taking on management responsibility for the whole device. Users keep their privacy, you keep your data. Everyone wins.

9. CONFIGURE EMAIL AUTHENTICATION: SPF, DKIM, DMARC

Without SPF, DKIM and DMARC properly configured, anyone in the world can send email "from" your domain, and some receiving mail servers will believe them.

That's how invoice fraud, supplier impersonation, and CEO fraud campaigns succeed. Fixing this protects your customers, your suppliers, and your domain reputation.

Self-assessment

- SPF record published in DNS, listing all legitimate senders (Exchange Online, marketing platforms, ticketing systems, etc.).
- SPF record uses -all (hard fail) once you're confident in the sender list.
- DKIM signing is enabled for all outbound mail in Exchange Online.
- DMARC record is published starting with p=none for monitoring, then p=quarantine, then p=reject.
- DMARC aggregate reports are received and reviewed regularly to identify unauthorised senders.
- Subdomains are covered (use sp= and explicit records for active subdomains).

What good looks like

Your domain is set to DMARC p=reject, with subdomains explicitly handled. Aggregate reports are reviewed monthly, and any unexpected senders are investigated. Spoofing attempts using your domain land in the spam folder of any decent inbox provider, or are bounced outright.

SFIT insight: This is the most common gap in the businesses we audit. Most have SPF, some have DKIM, and very few have DMARC enforced. While your DMARC is at p=none, spoofed emails using your domain are landing in your customers' inboxes today. The progression from p=none to p=reject takes weeks, not minutes start now.

10. BACK UP YOUR MICROSOFT 365 DATA

Microsoft's shared responsibility model is unambiguous: they keep the platform running, you keep the data safe. Microsoft does not back up your tenant against ransomware, malicious deletion, departing-employee sabotage, or rogue admin activity.

Native retention is short, recoverability is limited, and "we'll just call Microsoft" is not a recovery plan.

Self-assessment

- A third-party backup solution is in place (Veeam, Datto, Acronis, Keepit, etc.).
- Coverage includes Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Microsoft 365 Groups.
- Retention periods meet your business and regulatory requirements (typically 7 years for finance, longer for some sectors).
- Backups are stored in a separate security boundary from the production tenant.
- Restore tests are performed at least quarterly for individual items and for full mailboxes/sites.
- There is a documented restore process that someone other than the original engineer could follow.

What good looks like

A tested, recent restore not just a green tick on a dashboard. The backup product, retention, and restore processes are all aligned with the worst-case scenarios you actually face: ransomware, malicious deletion, departing employees, and accidental loss.

SFIT insight: We've recovered tenants from ransomware attacks where Microsoft's native retention had already expired by the time anyone noticed. Third-party backup with a tested restore is the difference between "incident" and "existential threat". If you take only one action from this guide, take this one.

COMMON MICROSOFT 365 SECURITY FAILURES

These are the issues that most often cause UK businesses to suffer Microsoft 365 incidents or to fail security audits. If any apply to your tenant, address them this quarter.

- MFA is enabled but not enforced for all users admin accounts or service accounts excluded.
- Legacy authentication remains enabled, allowing MFA to be bypassed entirely.
- No third-party backup of Microsoft 365 data relying on native retention only.
- Multiple standing global administrators, with no PIM or just-in-time elevation.
- Audit logging is disabled, or retention is set to the default to save costs.
- DMARC was published at p=none and never progressed leaving the domain spoofable.
- Defender for Office 365 licensed but not configured (no Safe Links, no Safe Attachments).
- Personal devices accessing company data with no Intune, no App Protection, no controls.
- No documented break-glass account, or one that's never been tested.

If three or more of these apply to your tenant, you have material exposure that an attacker can exploit today not in some hypothetical future scenario. These are the gaps that get businesses on the front page of the local newspaper.

SUGGESTED 30-DAY ACTION PLAN

If everything in this guide feels overwhelming, you're not alone most tenants get there over years, not weeks. Here is a realistic order of operations for getting from "exposed" to "defensible" in a single month.

Week 1: Stop the bleeding

- Enforce MFA on every account via Conditional Access.
- Disable legacy authentication tenant-wide.
- Confirm break-glass account exists, is tested, and is monitored.
- Enable unified audit logging if disabled.

Week 2: Lock down the admin layer

- Separate admin accounts from day-to-day accounts.
- Apply phishing-resistant MFA to all administrators.
- Review global admin assignments, remove anything stale.
- Configure PIM where licensing allows.

Week 3: Email and data protection

- Apply Defender for Office 365 preset security policies.
- Enable Safe Links, Safe Attachments, and impersonation protection.
- Publish DMARC record at p=none and start collecting reports.
- Deploy starter DLP policies for GDPR-relevant data.

Week 4: Devices and resilience

- Enrol devices in Intune (or accelerate existing rollout).
- Configure Conditional Access to require compliant devices.
- Validate third-party Microsoft 365 backup is in place and tested.
- Document everything, what's in place, who owns it, and when it's reviewed.

Following this plan won't get you to "perfect" security is never finished but it will close the gaps that attackers most reliably exploit, in the shortest practical timeframe.

HOW SYSTEM FORCE IT CAN HELP

Microsoft 365 security is not a one-off project. It's a continuous discipline that needs the right configuration, the right monitoring, and the right people watching the alerts. Most internal IT teams don't have the availability; most generic IT providers don't have the depth.

System Force IT delivers:

- Microsoft 365 security assessments tenant audit against this checklist and beyond.
- Conditional Access design and deployment, with proper testing and rollback planning.
- Defender for Office 365 and Defender for Endpoint configuration and tuning.
- Intune device management and Zero Trust device compliance.
- Email authentication (SPF, DKIM, DMARC) progression from p=none to p=reject.
- Third-party Microsoft 365 backup, with tested restore procedures.
- 24/7 monitoring of audit logs and security alerts, with an experienced team behind them.

Ready to harden your Microsoft 365 tenant?
Book a Microsoft 365 Security Review with System Force IT. One of our specialists will assess your tenant against all 10 actions in this guide, identify gaps, and provide a clear remediation plan with realistic timelines and costs.

- Book your free Microsoft 365 security review at systemforce.co.uk

Or call us directly: 01452 701355 We're based in Gloucestershire and work with businesses across the UK.

Authoritative sources and further reading

- Microsoft Security Documentation: learn.microsoft.com/en-us/security
- Microsoft 365 Zero Trust Guidance: learn.microsoft.com/en-us/security/zero-trust
- Microsoft Secure Score: security.microsoft.com (in your tenant)
- NCSC Cloud Security Guidance: ncsc.gov.uk/guidance/cloud-security
- NCSC Phishing Guidance: ncsc.gov.uk/guidance/phishing
- CISA Microsoft 365 Hardening: cisa.gov (Secure Cloud Business Applications)

This document is provided for general guidance only and does not constitute formal security or compliance advice. Microsoft 365 features, licensing, and product names change regularly; always verify against current Microsoft documentation before acting on specific recommendations.

System Force I.T.
Secure IT Simplified

Want a free Microsoft 365 security check with System Force IT?

We run free, no-obligation reviews for UK SMEs.
Written report in 7 working days.
No sales pitch, no follow-up unless you ask for one.

Book at systemforce.co.uk
Or call us directly: 01452 701355

System Force IT | supporting UK businesses since 2006.

UKAS ISO/IEC 27001: 2022 Certified | Microsoft Solutions Partner | Certified 3CX Partner | Cyber Essentials Practitioners | RIPE NCC Member

Next Step:

Book your free MICROSOFT 365 Security Quick Wins.

01452701355
www.systemforce.co.uk
sales@systemforce.co.uk