Microsoft 365 security hardening guide

Why default settings are not enough

- The Microsoft 365 system is a comprehensive platform to help small to medium-sized UK companies manage and store their emails/files and collaborate with their teams.
- Default settings offer convenience but lack the levels of security necessary for maximum safety.
- Default settings can create gaps in security and potential targets for hackers.
- In 2025, an estimated 43% of businesses in the UK experienced a cyber attack.
- Businesses who are required to comply with the UK GDPR also need to have safeguards in place to protect against unauthorised access to their customers' personal information.
- Poorly configured security settings can expose businesses to phishing scams, which are designed to steal user credentials and result in data breaches.
- Cyber Essentials, the UK government cybersecurity programme, provides guidelines to improve the security of systems against common threats through security hardening.
- Security hardening is the process of changing the way Microsoft 365 is set up so that it has increased levels of protection without losing ease of access.

What is Microsoft 365 security hardening?

In simpler terms, Microsoft 365 security hardening is about:

- Locking down your accounts
- Restricting access to risky (potentially compromising) areas
- Monitoring the activity on your (company's) accounts
- Preventing phishing attacks
- Controlling the sharing of sensitive data

Think of it as securing the doors and windows of a building.

The biggest Microsoft 365 risks for UK SMEs

- Credential Theft
- No Multi-Factor Authentication
- Legacy Authentication still in use
- Global Admin Overuse
- External Sharing Configuration Errors
- Email Impersonation
- Lack of Activity Monitoring
- No Back-up Capabilities

Step-by-step hardening checklist

The checklist follows a step by step order starting with Identity/Email, Data, and Monitoring. You can find what you need in either Microsoft 365 Admin Center (admin.microsoft.com) or the Security Portal (security.microsoft.com)

☐ Enable multi-factor authentication for all users.

☐ Disable legacy authentication protocols.

☐ Use Conditional Access Polices to block high-risk logins.

☐ Implement Least Privilege roles, no global admins for daily users.

☐ Protect admin accounts with dedicated logins and monitor them.

☐ Set up break glass emergency accounts.

☐ Implement anti-phishing policies in Defender for Office 365.

☐ Enable Safe Links and Safe Attachments.

☐ Implement anti impersonation rules.

☐ Restrict external forwarding.

☐ Limit external sharing in SharePoint/OneDrive.

☐ Enable link expiration(timed) and password protected links for shares.

☐ Manage guest access by performing regular reviews.

☐ Apply sensitivity labels to sensitive files.

☐ Enroll devices in Intune for management.

☐ Require devices to be encrypted and compliant.

☐ Enable Audit Logging and Retention.

☐ Implement Alert Policies for suspicious activity.

☐ Review Risky Sign-ins at least once per week.

☐ Monitor Admin Activity Changes.

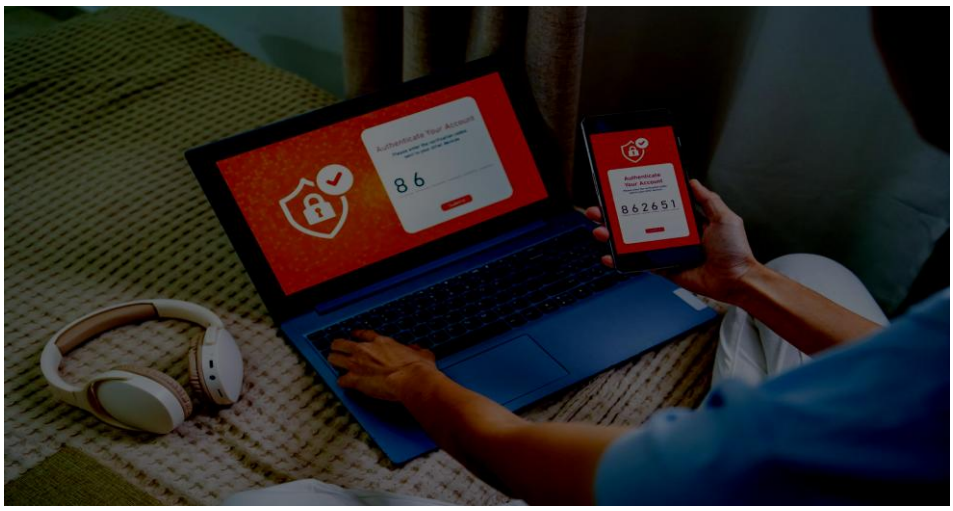
☐ Establish third-party backups for email and data.

☐ Implement Retention Policies for Auditing and Recovery.

Identity & Access Security

- MFA (multi-factor authentication) enforcement
- Conditional access
- Risks associated with legacy authentication
- Principle of least privilege
- Role-based administrative access

- Admin account protection checklist



Email & Phishing Protection

- Anti-phishing policy
- Safe links
- Safe attachments
- Anti-impersonation protection
- Block automatic forwarding
- Domain authentication (SPF, DKIM, DMARC)

SharePoint & OneDrive Security

- External sharing controls
- Guest access
- Link expiration
- Sensitivity labels
- File access auditing
- Accidental data exposure considerations

Device & Endpoint Integration

- Device compliance
- Encryption
- Patch management
- Conditional access from devices
- Microsoft Intune should be mentioned.

Logging, Monitoring & Alerting

- Audit Logging
- Suspicious Sign In Alerts
- Admin Activity Monitoring
- Security Alerts
- Describe the importance of log reviews.

Backup & Data Recovery

- Microsoft 365 Retention is NOT a Backup
- He importance of using a third-party Backup Solution
- Recovering from Ransomware
- Versioning & Retention Policies

Common configuration mistakes

- Not enabling multi-factor authentication.
- Leaving legacy authentication enabled.
- Allowing the use of external sharing.
- Not using conditional access policies.
- Ignoring alerts when administrators are attempting to take over accounts
- Assuming that data retention equals data backup.

30-60-90 day hardening roadmap

1-30 days: Create an initial foundation

- Enable security defaults and multi-factor authentication
- Disable legacy authentication
- Create conditional access policies (only allowing logins from the United Kingdom)
- Disable external sharing

31-60 days: Protection and monitoring

- Configure anti-phishing protections, safe links/attachments
- Implement DMARC/SPF/DKIM email filtering
- Enable auditing and alerts
- Enrol devices into Intune

61-90 days: Advanced and review

- Create and apply sensitivity labels to all documents
- Establish third-party backup systems
- Review risky sign-ins and monitor administrative activity
- Create security scorecard (ex. Microsoft Secure Score).

FAQs

1. Is Microsoft 365 automatic secured out of the box?

Yes however they will require configuration to enable many of the critical protections that exist.

2. Do we need additional security License?

Many of the advanced protections require you to be on a higher version of the Microsoft 365 security plans.

3. Is MFA enough?

MFA is certainly a key solution, however this should be combined with other controls that exist.

4. Is Small Business Targeted?

There are many attacks that are launched via automation that affect all types and sizes of organisations.

5. How often should we review our security settings?

Quarterly is a reasonable starting point for reviewing your current security settings.

About This Guide

The **Computer Support Centre** is an IT support and Cyber Security provider based in the UK. They assist small and medium sized businesses improve their security within their Microsoft 365 Platforms. The goal of this document is to provide solid, clear and uncomplicated advice to business owners, company directors and IT Managers who need to be assured that their Microsoft 365 infrastructure is secured appropriately. This document is not intended to be overly technical, but instead will help provide guidance on the most important configuration steps, common risks, and realistic controls that organisations can implement in order to reduce their cyber security risks, and protect their data.

If your company would like to complete a structured Microsoft 365 Security Assessment **Computer Support Centre** can review your current configuration and make specific recommendations for improvement, and ensure that your environment meets the best practice guidelines from the UK.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

While Microsoft 365 is generally regarded as an effective and secure system/platform, much of its security relies on proper deployment/configuration. Most security incidents affecting small- and medium-sized businesses occur due to non-sophisticated types of attacks, with the majority of incidents stemming from gaps in security, for example, not implementing multi-factor authentication (MFA), giving too many admin rights to employees or using too many open sharing settings).

Security hardening is about closing those gaps. By improving the overall protection for identities, email filtering, file sharing control, monitoring for suspicious behaviour and completing an adequate backup and recovery plan, UK SME businesses can reduce the likelihood of falling victim to phishing scams, ransomware and/or compromised accounts.

Security is not a one-time job. Conducting ongoing security reviews, providing staff with security awareness training and aligning your efforts with best practice recommendations like Cyber Essentials and the National Cyber Security Centre's guidance will ensure your Microsoft 365 environment remains resilient as your organisation scales.