# MICROSOFT 365 SECURITY CHECKLIST

**Secure Your Microsoft 365 Tenant in 10 Steps**

**Created by Jamola Cybersec Services Limited**

## INTRODUCTION

**Microsoft 365 is the backbone of many business operations, but it's also a prime target for cybercriminals. This checklist will help you secure your Microsoft 365 environment against common threats.**

## 10-STEP SECURITY CHECKLIST

### □ STEP 1: Enable Multi-Factor Authentication (MFA)

- Go to Azure AD > Security > Conditional Access
- Create policies requiring MFA for all users
- Exclude emergency access accounts carefully

### □ STEP 2: Configure Conditional Access Policies

- Implement risk-based conditional access
- Block access from high-risk sign-ins
- Require compliant devices for access

### □ STEP 3: Review and Improve Your Secure Score

- Check your Microsoft Secure Score in Microsoft 365 Defender
- Implement recommended actions
- Aim for a score of 80% or higher

### □ STEP 4: Configure Defender for Office 365

- Enable Safe Links and Safe Attachments
- Set up anti-phishing policies
- Configure spam and malware filtering

## □ STEP 5: Secure Email Communications

- Set up SPF (Sender Policy Framework)
- Configure DKIM (Domain Keys Identified Mail)
- Implement DMARC (Domain-based Message Authentication)
- Start with p=none policy, gradually move to p=reject

## □ STEP 6: Review SharePoint and OneDrive Sharing Settings

- Set default sharing to "Specific People"
- Enable external sharing only when necessary
- Review sharing links regularly

## □ STEP 7: Configure Identity Protection

- Enable user risk policies
- Configure sign-in risk detection
- Set up automated responses to risky behavior

## □ STEP 8: Implement Privileged Identity Management (PIM)

- Enable PIM for admin accounts
- Require justification for privilege elevation
- Set time limits for admin access

## □ STEP 9: Audit Logs and Monitoring

- Enable audit logging for all users
- Review audit logs regularly
- Set up alerts for suspicious activity

## □ STEP 10: Review and Enforce Compliance Policies

- Implement data loss prevention (DLP) policies

- Configure retention policies

- Ensure compliance with industry regulations

## EMERGENCY ACTIONS FOR A COMPROMISED ACCOUNT

Immediately block the compromised account

1. Reset the user's password

2. Revoke all sessions and tokens

3. Review audit logs for unauthorized activity

4. Report to Microsoft via Security & Compliance Center

## BEST PRACTICES

Regularly review and update your security configuration

- Test your security controls monthly

- Train users on security awareness

- Consider implementing a Zero Trust architecture

- Review permissions quarterly

## ABOUT JAMOLA CYBERSEC SERVICES LIMITED

Jamola Cybersec Services Limited provides remote cybersecurity services to SMEs worldwide. We help businesses secure their systems, protect their data, and build resilient security programmes.

Contact: info@jamolacybersec.uk

Website: https://jamolacybersec.uk