Syskit

Microsoft 365 Security Checklist

Domain	Do this first	What it prevents	How to verify
Identity	• Enforce MFA via Conditional Access • Limit Global Admins • Use cloud-only admin accounts • Enable PIM • Set up break-glass accounts	• Account takeover • Tenant compromise • Long-lived admin access • CA lockout	• Check sign-in logs for non-MFA auth • Review admin roles & PIM history • Test break-glass access
Email	• Enable Defender preset policies • Turn on Safe Links & Safe Attachments • Enable ZAP • Configure anti-phishing	• Phishing • Malware • CEO/CFO fraud	• Review threat explorer • Confirm policy coverage • Run test campaigns
Data	• Change sharing to "Specific people" • Enforce guest expiration • Enable DLP & sensitivity labels • Govern OAuth consents • Run access reviews	• Oversharing • Data exfiltration • Abandoned workspaces • Stale access	• Run sharing & guest reports • Check DLP events • Review OAuth consents • Confirm access reviews run
Devices	• Require compliant devices in CA • Define Intune compliance • Apply app protection for BYOD • Enable ASR rules	• Compromised endpoints • Unmanaged device access • Malware execution	• Verify CA device conditions • Review compliance reports • Confirm policy deployment
Monitoring	• Enable unified audit logging • Tune Secure Score • Extend audit retention • Back up tenant config	• Configuration drift • Incomplete investigations • Weak audit evidence	• Check & track Secure Score • Validate audit events • Confirm retention period • Test config restore