Microsoft 365 Security Best Practices

A practical Microsoft 365 checklist for identity, email, devices, and data protection.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.

Why Microsoft 365 Security Matters

Microsoft 365 is where many businesses store email, files, collaboration activity, and identity access. Securing Microsoft 365 helps protect the front door to the business.

Quick-Win Security Checklist

Done	Security Item	Why It Matters
[ ]	Require MFA for all users, especially administrators.	MFA helps protect accounts when passwords are phished or reused.
[ ]	Use Security Defaults or Conditional Access based on licensing and business needs.	Baseline controls help reduce common identity-related attacks.
[ ]	Block legacy authentication where possible.	Legacy protocols can bypass stronger authentication controls.
[ ]	Protect administrator accounts with least privilege.	Admin accounts should be limited, monitored, and used only when necessary.
[ ]	Enable audit logging and review sign-in activity.	Logs help identify suspicious access and support investigations.
[ ]	Configure email authentication: SPF, DKIM, and DMARC.	These controls help reduce email spoofing and impersonation risk.
[ ]	Use anti-phishing and impersonation protection.	Many attacks start with a convincing email.
[ ]	Control external sharing in SharePoint and OneDrive.	Sharing should be intentional, reviewed, and limited to business need.
[ ]	Protect devices accessing company data.	Managed devices reduce exposure from lost or unmanaged endpoints.
[ ]	Maintain off-platform backups for critical Microsoft 365 data.	Retention and backup are different. Recovery planning should be intentional.

Admin Review Questions

- Who has Global Administrator access and why?
- Are inactive user accounts disabled quickly?
- Are mailbox forwarding rules reviewed for suspicious destinations?
- Are users trained to report phishing from Outlook or Teams?
- Is there a written process for terminating employees and removing access?

Helpful Reference Points

- Microsoft Learn states Security Defaults include MFA registration, MFA for administrators, MFA when necessary, blocking legacy authentication, and protecting privileged activities.
- Microsoft Learn recommends using least-privileged roles and notes that Security Defaults and Conditional Access are common approaches to MFA in Microsoft 365.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com