



Harbour IT

RECOMMENDED PROJECTS

Northwind Traders

PREPARED BY

Harbour IT

DATE

12 October 2026

BASED ON

Your Microsoft 365 settings, read-only

MICROSOFT 365 TENANT

northwindtraders.onmicrosoft.com

IN THIS REPORT

Identity and Conditional Access	2
Email security	2
Device management with Intune	3
Windows upgrade and hardware refresh	3

Summary

We reviewed your Microsoft 365 settings and recommend 4 projects, most urgent first. Each one lists what we found and what the work covers.

1. Identity and Conditional Access

● High

Most break-ins start with a stolen password, and admin accounts are the biggest prize. Requiring a second factor everywhere, blocking the old sign-in methods that can't ask for one and locking down admin accounts stops nearly all of them.

WHAT WE FOUND

- Legacy authentication is allowed
- 14 users without MFA
- 1 guest with admin roles
- 1 admin not covered by MFA
- Enforced by Require MFA for all users, with 1 exclusion to review
- 1 app with privileged roles
- 2 admins without a phishing-resistant method
- 3 people can only use a text or call as a second factor

WHAT THE PROJECT COVERS

- Conditional Access policies: MFA for everyone, legacy sign-in blocked, break-glass accounts
- MFA registration drive, moving people off text and call codes to the Authenticator app
- Admin accounts: the right number of Global Administrators, cloud-only, phishing-resistant sign-in
- Risky sign-in and risky user handling
- Report-only rollout first, so nobody is locked out

Scope: 36 users

2. Email security

● High

Email is how most attacks arrive and how fraud gets paid. Locking down the domain stops others pretending to be the business, and closing forwarding and old protocols stops mail leaking out.

WHAT WE FOUND

- 4 external forwards
- 1 suspicious inbox rule
- 2 domains without DMARC enforcement
- 1 mail domain without DKIM
- 1 domain with SPF problems
- 1 of 1 mail domain doesn't fully enforce MTA-STS
- SMTP AUTH is on for the organisation

WHAT THE PROJECT COVERS

- SPF, DKIM and DMARC set up and enforced for every domain
- Encrypted delivery (MTA-STS and TLS reporting)
- External forwarding and suspicious inbox rules removed and blocked
- SMTP AUTH turned off, mailbox auditing on, shared mailboxes locked

Scope: 40 mailboxes

3. Device management with Intune

● High

Company data lives on laptops and phones. Managing them means they're encrypted, kept up to date and can be wiped if lost, and unmanaged devices can be kept away from company data.

WHAT WE FOUND

- 4 of 36 computers not encrypted
- 6 of 37 managed devices not compliant
- 1 of 37 joined computers not in Intune
- 3 devices haven't checked in for 30+ days
- 1 of 39 device records unused for 90+ days

WHAT THE PROJECT COVERS

- Intune enrolment for every company computer (Autopilot for new ones)
- Compliance policies: encryption, updates, antivirus, screen lock
- BitLocker with recovery keys stored in Entra ID
- Clean-up of old devices

Scope: 39 devices

4. Windows upgrade and hardware refresh

● High

Computers on a Windows version that no longer gets security updates stay open to every flaw found from now on. Upgrading, or replacing machines that can't upgrade, closes that gap.

WHAT WE FOUND

- 5 of 36 Windows computers past end of support

WHAT THE PROJECT COVERS

- Which computers can upgrade in place and which need replacing
- Upgrades scheduled around the working day
- Replacement hardware quoted and set up

Scope: 5 computers

Next steps

We'd be glad to talk through any of these and put together a quote.

Harbour IT · help@harbourit.example · 0161 496 0000