Microsoft 365 Security Hardening (Mini Project)

Report

Overview:

This mini project demonstrates the implementation of key Microsoft 365 security configurations in a

Microsoft 365 E5 developer tenant. It focuses on enabling Security Defaults for MFA, designing

Conditional Access and device compliance plans, and reviewing Microsoft Defender for Office 365

protections. The goal was to establish a secure identity and access baseline aligned with

Microsoft's Zero Trust principles.

Objectives:

- Enable and verify Security Defaults for MFA and legacy authentication blocking.
- Design a Conditional Access policy requiring MFA for admins.
- Plan a device compliance policy for secure device management.
- Capture sign-in logs to confirm MFA enforcement.
- Review and document Defender for Office 365 anti-phishing and Safe Links policies.

Area	**Configuration / Outcome**
Identity Protection	Enabled Security Defaults to enforce MFA and block legacy authentication.
Conditional Access	Planned 'Require MFA for Admins' policy.
Device Compliance	Planned Intune compliance policy requiring encryption and PIN.
Defender for O365	Reviewed default anti-phishing and Safe Links configurations.
Audit Logs	Captured sign-in logs confirming MFA enforcement.

Results:

The Microsoft 365 tenant successfully enforced MFA for all users through Security Defaults.

Although the sandbox environment limited Conditional Access and Intune configurations, documented policy designs demonstrate knowledge of enterprise-grade security practices. Audit

logs verified MFA prompts during user sign-in events, achieving the project’s objectives.

Skills Demonstrated:

- Microsoft 365 Identity and Access Management
- Multi-Factor Authentication (MFA) configuration
- Conditional Access & Device Compliance planning
- Microsoft Defender for Office 365 configuration
- Documentation and GitHub portfolio management

Repository:

https://github.com/chardii95/M365-Security-Hardening