CMMC

IDENTIFICATION & AUTHENTICATION

Prove it's you, every time.

IA makes sure users, devices, and services are who they say they are before they ever touch your systems or data. It's about strong logins, smart verification, and shutting down impostors so your real team can work fast and safely.

Proof of Practice

Examples

- **Identity & Device Inventory**
  Screenshot(s) showing all users, privileged roles, and managed devices with owner, last sign-in, compliance status, and review date.
- **Conditional Access Review**
  Screenshot of policy set requiring MFA and blocking risky sign-ins; notes on exceptions and last review date.
- **Password Policy Review**
  Screenshot of tenant password settings and password protection (ban list/lockout), with date captured.

The Business Impact

A 40-person machine shop won a rush order, then an ex-employee's still-active account let attackers reset an admin password. Email was locked, drawings leaked, and the prime paused the PO for two weeks. Simple IA fixes would've saved revenue, reputation, and trust.

Available Resources

- **NIST SP 800-63 Digital Identity Guidelines**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- **CISA "Implementing Strong Authentication"**
  https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508_1.pdf
- **Microsoft Entra ID**
  https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id
- **LastPass**
  https://www.lastpass.com/
- **1Password**
  https://1password.com/

Quick Wins

1. Turn on MFA everywhere
2. Kill shared logins and give every person their own account
3. Enforce strong passwords (length + password manager)
4. Disable dormant accounts older than 30 days
5. Add just-in-time admin access instead of always-on privileges

CyberNEX Technology