Explain Password Best Practices



Phil Chapman
Senior Instructor and Subject Matter Expert

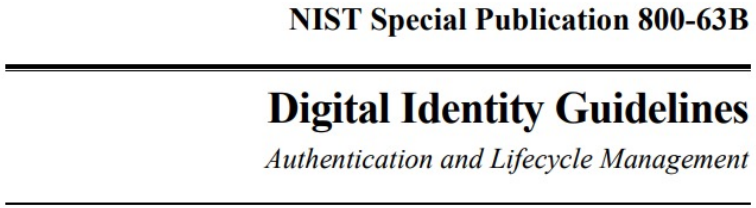
www.cyberphil.co.uk

Understanding Password Security



What is a password?

- Something that you know
- Authentication factor
- Memorized secret (NIST)
  - Password or PIN



NIST Special Publication (SP) 800-63B

Digital identity guidelines

- Memorized secrets to be at least 8 characters
- All ASCII characters allowed
  - If chosen by the user
- Memorized secrets to be at least 6 numbers
- Randomly generated
  - If chosen by the credential service provider

Password123
AlreadyCompromised
AAAAA1111
Microsoft123

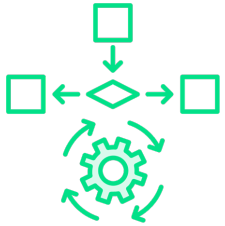
Passwords should not be:

- Dictionary words
- Obtained from previous breaches
- Repetitive or sequential characters
- Context specific (company name, username, service etc)

Length and Complexity



Passwords should be long - depending upon the assessed threat



Complexity (mixture of letters, numbers and special characters) should be used



Highly complex passwords are a potential vulnerability!

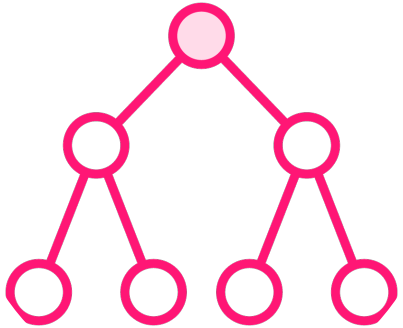
Password Attacks



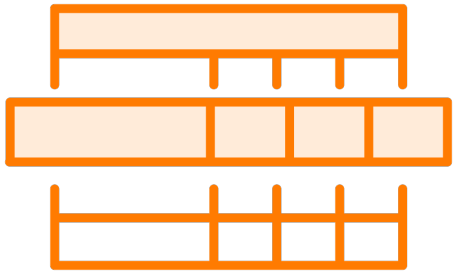
Guessing



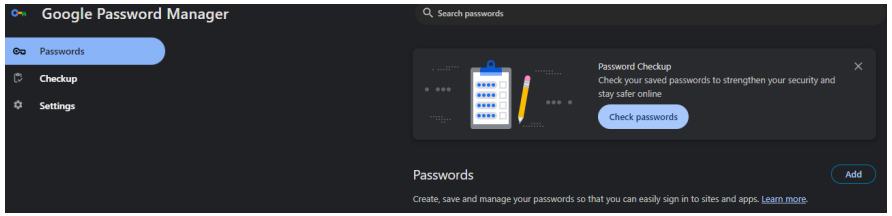
Brute force

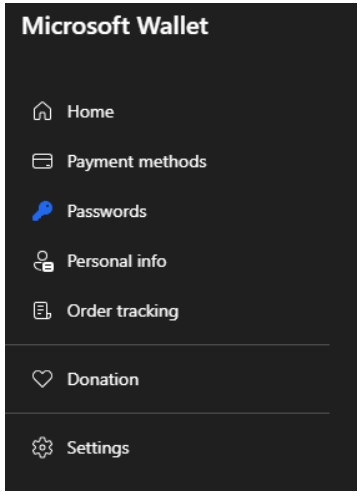


Credential stuffing



Rainbow table





Password managers

- Used to assist users to generate strong passwords
- Automatically generate length and complexity
- Automatically set expiration time (if required)
- Automatically layer in MFA

Up Next:

Administering Password

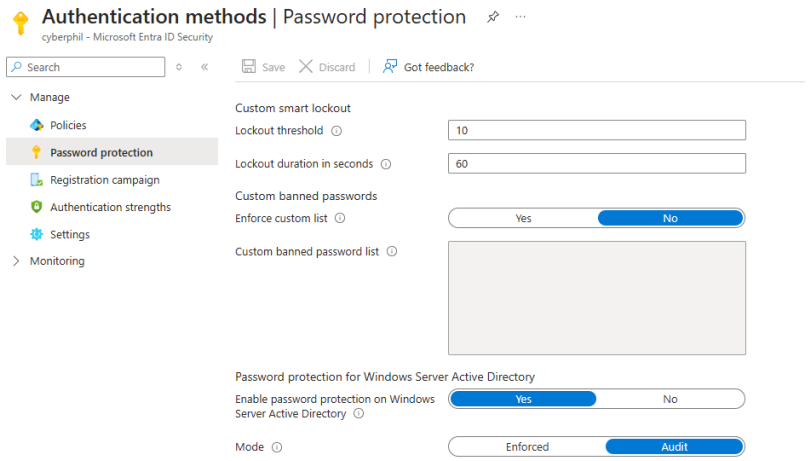
Administering Passwords



Password policies

Policy determines the following:

- Minimum length
- Complexity requirements
- Expiry
- Lockout thresholds
- MFA



Password policy controls

- Enforced by Group Policy (GPO)
  - Local and domain-based networks
- Cloud-based Identity and Access Management (IAM)

Password Reset Process



User forgets their password (account is locked)



Forced reset due to security breach



Automatic reset due to security alert



Self service reset



Password security best practice

- Never use the same password
- Long and complex
- Use password managers
- Always change default usernames and passwords
- Enable MFA

Up Next:

Identify Common Use Cases for Encryption