Cybersecurity

4.6.3 – Passwords

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Password Best Practices

- Length
  - Longer is generally more secure
  - Makes brute-force attack more difficult
- Complexity
  - Mix of uppercase, lowercase, numbers, and special characters
  - Reduced likelihood of brute-force or dictionary attacks
- Reuse
  - Don’t reuse passwords across accounts
  - Do use unique passwords for different services
- Expiration
  - Implement expiration policies
  - Regularly changing passwords mitigates impact of credential compromises
- Age
  - Restrict use of old potentially compromised passwords

Password Managers

- These are tools or applications that help users
  - Generate, store, and manage unique passwords
  - Support for multiple accounts
  - Enhance security by eliminating the need for users to remember complex passwords
- Benefits
  - One master password per vault
  - Easy to access all user accounts
- Drawbacks
  - If the manager is compromised, then malicious actors could access accounts associated with the manager.

Passwordless

- Eliminates the need for traditional passwords
- Relies on alternative authentication methods
  - Biometrics
  - Security keys
  - One-time codes
- Benefits
  - Enhanced security by reducing reliance on passwords
  - Reduces the risk of password-related attacks
  - Alternative authentication processes can be user-friendly