Online Protection

Also see Social Networking & Doxxing and Online Privacy.

Reference

- https://www.cisa.gov/secure-our-world
- https://www.cisa.gov/topics/cybersecurity-best-practices
- https://www.techlore.tech/resources
- https://cure53.de

Credit Report

- **Freeze credit report**
  - Free service from credit agencies
    - Can be “frozen and unfrozen” immediately at anytime.
    - https://www.usa.gov/credit-freeze

Passwords

- **Use a strong password**
  - https://www.cisa.gov/secure-our-world/use-strong-passwords
- **Use a password manager**
  - Bitwarden - https://bitwarden.com (cloud-based)
  - Keepass - https://keepass.info (Local storage)
- **Use a different password for each account**
  - If a hacker gets one password, they can try the same password for other accounts.
- **Use Multifactor authentication (MFA) or Two factor authentication (2FA)**
  - Use the app version recommended by the vendor
  - Text message (SMS) method is not recommended and less secure

Quantum-Resilient Password Lengths

As of May 2025

Password Use Case	Recommended Length (Post-Quantum)	Notes
Standard login password (hashed with bcrypt/scrypt/Argon2)	16+ characters	Include upper/lowercase, numbers, symbols. Use a passphrase (e.g., “CorrectHorseBatteryStaple”).
High-security systems (admin, financial, sensitive data)	20–24+ characters	Use passphrases or random strings from a password manager.

Password Use Case	Recommended Length (Post-Quantum)	Notes
Encryption passphrases (e.g., PGP, file encryption)	32+ characters	Quantum attacks may eventually brute-force shorter keys; longer passwords help mitigate risk.
Wi-Fi passwords (WPA3)	16–24 characters	Use maximum supported length to reduce offline cracking potential.