

Password Policy Practical Implementation

Use MFA wherever you can

Multifactor Authentication where you can to protect valuable things

Whenever possible use phishing-resistant MFA

<https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa>

Use MFA and/or long passwords/passphrases to logon to your devices

All passwords should be changed at least annually

For ↓ Passwords

If you can, use a Password Manager

Protect password manager with MFA and/or long password/passphrase

12-character perfectly random passwords defeat all known guessing/cracking attacks

Perfectly Random Password Examples

R#Yv&ZCAojrX
ELv!2MibAb>RC?ru
a!#=dH)vvLykiJhu

If you must create a password

Create a unique, different, long password/passphrase for all sites and services

Human-created passwords
8-characters - weak
12-characters - better
20-characters - strong

Examples of Good Passphrases

I went to 7-11 earlier today.
rogerjumpedoverthepurplefox
2belivingtherockandrolllifeforever

*Hackers are routinely cracking 18-character human-created Windows passwords if they get the hashes

Optimally:

MFA +
Password Manager +
Strong individual passwords where needed

For more detail: <https://info.knowbe4.com/wp-password-policy-should-be>