ManageEngine
ADSelfService Plus

BEST PRACTICES GUIDE TO PASSWORD SECURITY

Passwords are the first line of defense against cyberattacks, so it's important for individuals and organizations to make password security a priority. Many of us either don't take it seriously, or are unaware of the recommended steps to follow.

This infographic
helps you create and manage strong passwords,
and **keep your accounts safe**

DO'S

ALWAYS CHOOSE A STRONG AND UNIQUE PASSWORD

Passphrases are considered strong and unique compared to the algorithmic password complexity requirements. Make sure your password is both long and complex.

Example: A 12-character password with a mix of uppercase and lowercase letters, numbers, and symbols takes 62 trillion times longer to crack than a password with just six lowercase letters.

USE A PASSWORD MANAGER

Password managers generate complex passwords for you and save them using encryption, so you don't have to remember them. Find yourself a right solution and ease your password management.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Don't rely solely on passwords for security. Add additional layers of security using biometric authentication, or an authenticator app.

CHANGE PASSWORDS ONLY WHEN NECESSARY

Periodic password changes are not recommended by NIST as they have no impact on password security. Password-based attacks have more to do with weak or bad passwords, and very little to do with password age. Change your password only if you suspect your account has been compromised. Also, change the default passwords on hardware and applications to something more secure.

SET RESTRICTIONS FOR THE NUMBER OF FAILED LOGIN ATTEMPTS

Set a minimum of five failed password attempts before a user is locked out of a system or service. This way, you can prevent brute-force attacks.

DONT'S

DO NOT USE EASILY GUESSABLE INFORMATION

Avoid using personal information such as your birthdate, phone number, or family members' names as your password. Use a password manager that prevents you from using dictionary words.

DO NOT REUSE THE SAME PASSWORD ACROSS MULTIPLE ACCOUNTS

The logic is simple—if one of your passwords is stolen, cybercriminals can use it to breach all the connected accounts. Reusing passwords is a security risk best avoided.

DO NOT STORE PASSWORDS IN UNSECURE LOCATIONS

Do not store your passwords in plain text in the notes app on your phone, a spreadsheet on your computer, or on sticky notes.

AVOID USING REPETITIVE OR INCREMENTAL PASSWORDS

When your password expires, or you are advised by a security team to change the password, change it to a strong and unique one. Changing "Passwor"d to "P@ssw0rd" or "Password1" will rarely make any difference to your security.

DO NOT LOGIN TO UNSECURED NETWORKS

Do not connect to Wi-Fi networks in unknown or random places, as they're more vulnerable. Always use mobile data in such instances, and avoid accessing sensitive data while using public networks.

Analyze your password knowledge

TAKE THE PASSWORD QUIZ

Adopt password best practices and **enhance password security** with **MangeEngine ADSelfService Plus**

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus

SCHEDULE A DEMO