National Cyber Security Centre

Password Policy
Advice for system owners

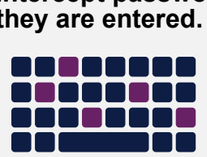
The NCSC is working to reduce organisations' reliance on users having to recall large numbers of complex passwords. The advice below advocates a greater reliance on technical defences and organisational processes, with passwords forming just one part of your wider access control and identity management approach.

How passwords are discovered...

Interception
Passwords can be intercepted as they travel over a network.

Brute force
Automated guessing of billions of passwords until the correct one is found.

Key logging
Installing a keylogger to intercept passwords when they are entered.



Manual guessing
Details such as dates of birth or pet names can be used to guess passwords.

Shoulder surfing
Observing someone typing in their password.

Stealing passwords
Insecurely stored passwords can be stolen, such as ones written on sticky notes and kept near (or on) devices.

Stealing hashes
Stolen hash files can be broken to recover the original passwords.

Phishing & coercion
Using social engineering techniques to trick people into revealing passwords.

Data breaches
Using the passwords leaked from data breaches to attack other systems.

Password spraying
Trying a small number of commonly-used passwords to access a large number of accounts.

...and how to improve system security.

Reduce your reliance on passwords
1. Only use passwords where they are needed and appropriate.
2. Consider alternatives to passwords such as SSO, hardware tokens and biometric solutions.
3. Use MFA for all important accounts and internet-facing systems.

Implement technical solutions
1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before locking out.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Protect all passwords
1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Chose services and products that protect passwords using standards such as SHA-256.
4. Protect access to user databases.
5. Prioritise administrators, cloud accounts and remote users.

Help users generate better passwords
1. Be aware of different password generation methods.
2. Use built-in password generators when using password managers.
3. Don't use complexity requirements.
4. Avoid the creation of passwords that are too short.
5. Don't impose artificial capping on password length.

Key messages for staff training
1. Emphasise the risks of re-using passwords across work and home accounts.
2. Help users to choose passwords that are difficult to guess.
3. Help users to prioritise their high value accounts.
4. Consider making your training applicable to users' personal lives.

Help users cope with password overload
1. Allow users to securely store their passwords, including the use of password managers.
2. Don't automatically expire passwords. Only ask users to change their passwords on indication or suspicion of compromise.
3. Use delegation tools instead of password sharing. If there's a pressing business requirement for password sharing, use additional controls to provide the required oversight.