SOCONNECT™
inspired communications

PASSWORD POLICY

KEEPING YOUR DATA SECURE

One of the primary protections when it comes to keeping data secure is the humble password. Attackers use various techniques to discover passwords, which include using powerful tools available for free on the internet. However, on many occasions, a powerful tool would scarcely be needed, with the most commonly used (and woefully inadequate) passwords being the easiest and quickest to crack.

How attackers crack passwords:

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.

Social Engineering
Using social engineering techniques to trick people into revealing passwords.

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

Interception
Attackers can intercept passwords as they are transmitted over a network.

Password Theft
Passwords stored insecurely are easily stolen – this includes handwritten passwords hidden close to a device.

By Force
Automated guessing of billions of passwords until the right one is found.

Password Spraying
Lists of a small number of common passwords are used to brute force large numbers of accounts

Key Logging
An installed keylogger can intercept passwords as they are typed.

How to avoid a password attack:

Use Technical Controls
1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before the account is frozen.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Reduce your business's 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.

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.

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 to 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.

soconnect.co.uk ✉ sales@soconnect.co.uk ☎ 0333 240 1824