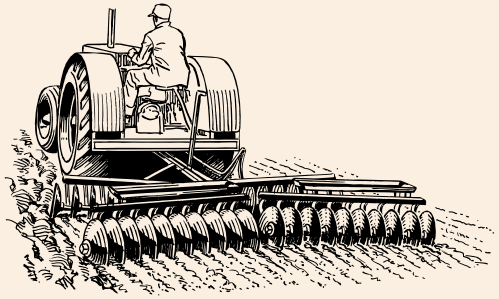
Password FAQ's



Password FAQ's

Q: Why do I need a strong password?

Strong passwords protect your accounts from hackers. Weak passwords can lead to financial loss and data breaches.

Q: What makes a password strong?

A strong password is at least 12 characters long, uses a mix of letters, numbers and symbols. It also avoids common words, phrases and dates.

Q: Should I use the same password for multiple accounts?

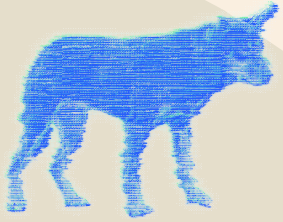
No. Using a unique password for each account will improve security overall. It's like having a different set of keys for your shed, house, tractor and ute.

Q: How do I remember all of my passwords?

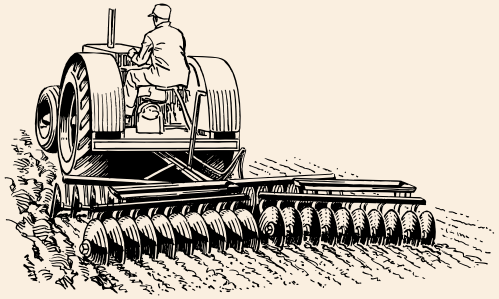
·Use a password manager to store and manage your login details securely. Many can also generate strong passwords for you.

How can I protect my passwords from phishing attacks?

·Don't trust emails asking for your password. Verify the sender, avoid suspicious links and use 2FA/MFA for added security.



Password FAQ's



Password FAQ's

Q: How often should I change my password?

Change passwords on a regular basis, especially if the account has been compromised.

Q: What should I do if my password has been compromised?

·Change it immediately and check for suspicious activity. You should also change the password for any account that uses the same combination of email/username and password. Consider enabling 2FA/MFA if available.

Q: Are password security questions safe?

Yes, but avoid easily guessed answers. Consider using a false answer that only you know.

Q: What is a passphrase?

·A passphrase is a longer, sentence like password that is easier to remember and harder to guess. Eg. OldDogSleepsAllDay

Q: What is 2FA/MFA?

·2FA/MFA is like added security. It requires multiple forms of verification to access your account, making it much harder for hackers to gain access.