PASSWORD SECURITY

1 IMPORTANCE OF USING STRONG PASSWORDS

Weak passwords can be guessed easily or cracked by hackers. This can lead to potential financial losses, identify theft, and privacy breaches.

2 WHAT MAKES A STRONG PASSWORD?

- Is at least 12 characters long.
- Includes a mix of uppercase and lowercase letters, numbers and special characters.
- Avoids common words, phrases or contains easily guessable things such as birthdays or names

3 USE A UNIQUE PASSWORD FOR EACH ACCOUNT

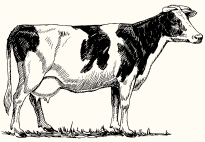
You should use a unique password for each online account. This way, if one account is compromised, it won't affect other accounts. It's just like a different set of keys for the ute, tractor and shed.

4 PASSWORD MANAGERS

Use a password manager. They are a great way to store and manage your login credentials for different online accounts. They can even generate unique and complex passwords automatically for you.

5 2FA AND MFA

2FA and MFA add an extra layer of security by requiring two or more verification methods to access your account. This might include something you know, such as a password, something you have, like a mobile phone, and something you are, like your fingerprint.



UPLIFTING FARMERS' CYBER SECURITY AWARENESS

PASSWORD SECURITY

6 YOUR PASSWORD HAS BEEN COMPROMISED

Change it immediately. Also check the affected account for any suspicious activity. If possible, enable 2FA or MFA authentication. It's a bit like fixing your fence when it's broken.

7 PASSWORD SECURITY QUESTIONS

Security questions can help add a layer of security but can also lead to a data breach if chosen poorly. Avoid questions that could be easily guessed or found online through social media accounts. You could consider using false answers such as my favourite animal is tractor.

8 PASSPHRASES

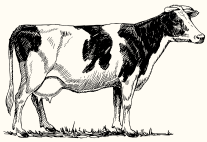
A passphrase is like a sentence or sequence of words that is longer than a typical password. The benefit of them is they are easier to remember, and still difficult to guess.

9 PROTECT YOUR PASSWORDS FROM PHISHING?

Never trust emails or messages asking for your password. Always verify the sender identity and avoid clicking any suspicious links. Use 2FA or MFA as an added layer of security.

10 CHANGING YOUR PASSWORD

It's good practice to change your passwords on a regular basis, especially if they may have been compromised. Avoid common practices such as incrementing the first or last character of the same password. eg abc2 to abc3 to abc4.



UPLIFTING FARMERS' CYBER SECURITY AWARENESS