AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

PASSWORD MANAGEMENT

PROTECT YOUR INFORMATION

WHAT IS PASSWORD MANAGEMENT?

Password Management is the practice of creating, storing, and handling passwords securely to protect your online accounts from unauthorised access. Passwords are often the first line of defence; therefore, strong password management practices are essential to reduce the risk of security breaches and identity theft.

Example: Rather than using simple, easily guessed passwords or the same password across multiple accounts, password management involves using complex, unique passwords for each account and storing them securely.

+61 2 5105 1022 | info@aada.asn.au | www.aada.asn.au/cyber-security-dashboard/

CULTURAL CYBER SECURITY

THREATS

Poor password management can leave you vulnerable to a range of cyber threats, as passwords are often a primary target for hackers looking to gain access to accounts and systems.

Key Risks:

- If attackers gain access to your password, they can take control of your accounts, leading to data theft, financial loss, or impersonation.
- Weak or reused passwords make it easier for attackers to compromise systems, which can result in data breaches that expose sensitive information.
- Stolen passwords can provide criminals with access to personal information, allowing them to impersonate you and commit fraud.

TIPS

To practice good password management it is important to:

- Create strong passwords with a mix of characters and change them regularly.
- Never share passwords.
- Avoid using the same password on multiple sites.
- Do not base passwords on personal information.
- Enable Multi-Factor Authentication.
- Use a password manager.
- Avoid saving passwords in browsers.
- Be cautious with security question answers.
- Use a password strength chart to evaluate your passwords. This helps identify weak passwords that need strengthening to improve security.
- Visit Have I Been Pwned to check if your information has been compromised in a data breach. If any of your accounts are exposed, update those passwords immediately.
- Avoid syncing passwords across multiple devices, as this can increase vulnerability if one device is compromised. Stick to secure storage options, like a dedicated password manager, for enhanced security.