AADA
AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

SOCIAL ENGINEERING

PROTECT YOUR INFORMATION

WHAT IS SOCIAL ENGINEERING?

Social engineering is a method used by cybercriminals to trick people into revealing confidential information or taking actions that compromise security. Instead of hacking technology, social engineering targets human psychology. Criminals might pretend to be a trusted individual, like a company representative, family member, or coworker, and persuade you to share information or access sensitive areas.

Example: A stranger contacts you on social media, pretending to be a friend of a mutual acquaintance. They gradually build trust over several messages, eventually asking you for personal information like your address or workplace, claiming they need it for a surprise or to send you something special. In reality, they are using the friendly approach to gather sensitive details about you.

THREATS

Social engineering attacks can lead to unauthorised access, data theft, financial loss, and compromised security systems. Because social engineering exploits trust, these attacks are often difficult to detect, making them particularly dangerous for individuals and organisations alike.

Key Risks:

- Attackers gain access to sensitive accounts or data by tricking someone into granting them access.
- Scammers may use social engineering to steal confidential information, such as company secrets or personal information.
- Social engineering can result in significant financial losses and can damage an individual's or organisation's reputation if information is leaked or misused.

TIPS

To prevent falling victim to social engineering it is important to:

- Be skeptical of sudden requests for sensitive information, even if the person claims to be in a position of authority. Verify their identity through a trusted source before responding. This can include fake e-mails from staff asking to change their bank account details for the next payrun. Always call the person to verify these changes.
- Regularly educate yourself on common social engineering tactics and participate in any training programs offered to increase awareness.
- Use Multi-Factor Authentication.
- Keep your software and systems up-to-date to protect against vulnerabilities that attackers might exploit.
- Avoid sharing personal or sensitive details on social media or other public platforms, as attackers may use this information to make their scams more convincing.