AADA AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

PHISHING

PROTECT YOUR INFORMATION

WHAT IS PHISHING?

Phishing is a type of online scam where criminals pretend to be legitimate companies or people you trust, like a bank, online store, or even a coworker. They usually send emails, messages, or create fake websites to trick you into sharing personal information, like passwords or credit card details. Phishing can also happen through phone calls or text messages.

Example: You get an email that looks like it is from your bank, asking you to confirm your account details. But, the email is actually from a scammer trying to steal your information.

THREATS

Phishing attacks are dangerous because they can lead to identity theft, financial loss, and security breaches. When someone falls for a phishing scam, criminals can access sensitive information, misuse accounts, or even infect devices with harmful software. Phishing attacks often target individuals, but they can also affect entire businesses if an employee accidentally shares company details.

Key Risks:

- Criminals can use stolen information to make unauthorised purchases, steal funds, or commit credit card fraud.
- Phishers can use personal information to impersonate victims.
- Phishing attackers can trick victims into clicking a malicious link that installs malware on their device.

TIPS

To prevent phishing attacks it is important to:

- Be cautious with unexpected emails, especially those asking for personal information or containing urgent language.
- Avoid clicking on links in unexpected emails or messages, even if they look familiar. Hover over links to see where they lead.
- Always check the sender’s email address or phone number. Look out for small errors that might signal a fake.
- Use Strong, Unique Passwords, a password manager and enable Multi-Factor Authentication.
- Many email providers and messaging platforms allow you to report phishing attempts. Reporting helps to prevent scams from spreading.