AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

CYBER SECURITY HYGIENE

PROTECT YOUR INFORMATION

WHAT IS CYBER SECURITY HYGIENE?

Cyber security hygiene refers to the routine practices and habits that help keep your devices, data, and networks secure from cyber threats. Just as personal hygiene protects your health, cyber hygiene protects your digital security. By maintaining good cyber hygiene, you reduce the chances of falling victim to cyberattacks, data breaches, and malware infections.

Example: Regularly updating software, using strong passwords, and being cautious about suspicious links are part of good cyber hygiene. These habits help protect your data and reduce your vulnerability to cyber threats.

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

CULTURAL CYBER SECURITY

THREATS

Neglecting cyber hygiene can leave systems and devices vulnerable to a variety of cyber threats, potentially resulting in data loss, identity theft, financial loss, and unauthorised access to personal or corporate accounts.

Key Risks:

- Outdated software or lack of antivirus protection can make your device susceptible to malware, such as viruses, ransomware, and spyware.
- Weak passwords and lack of encryption make it easier for hackers to access and steal sensitive information.
- Poor password management and lack of multi-factor authentication (MFA) can lead to unauthorised access to personal and work accounts.
- If cybercriminals access your personal information, they can impersonate you, potentially causing financial and reputational damage.

TIPS

To practice good cyber security hygiene it is important to:

- Always update your operating system, apps, and security software. These updates include security patches that protect against new threats.
- Create strong passwords using a mix of letters, numbers, and symbols. Avoid reusing passwords across different accounts. Consider using a password manager to keep track of complex passwords securely.
- Enable Multi-Factor Authentication to your accounts provides an extra layer of security, so even if someone has your password, they will need an additional form of verification.
- Protect your devices with trusted antivirus software and run regular scans to detect hidden threats.
- Enable a SPAM filtering software to detect Illegitimate emails before they reach your inbox. Users or IT staff can log into the system and release legitimate emails that might get caught.
- Avoid clicking on links or downloading attachments from unknown sources, as these could be phishing attempts or malware.
- Regular backups to an external drive or cloud storage are crucial. This way, you can recover important files if an attack occurs.
- Be mindful of what you share publicly on social media, as attackers may use this information for social engineering.
- Use Secure Wi-Fi Connections and avoid public Wi-Fi for sensitive activities like online banking. If you must use public Wi-Fi, a VPN can help secure your connection.

+61 404 492 220 | enquiries@culturalcybersecurity.com | www.culturalcybersecurity.com