New South Wales Branch
PO Box 277
HURSTVILLE NSW 2220
Tel: 0412 880861
Fax: 02 9579 2333
Email: hughmc@artionsw.com.au

ARTIO
Australian Road Transport Industrial Organisation

The Courier

Information and Advice for NSW Transport Operators

Newsletter Vol. 6 No 10, 17 April, 2020

Contents

COVID-19: NHVR Develops New Online Truck Stop Tool

Adapted from media release, National Heavy Vehicle Regulator CEO, Sal Petrocitto, 9 April, 2020

The NHVR has launched a new online tool that maps service centres, truck stops and roadhouses that remain open for heavy vehicle drivers.

NHVR CEO Sal Petroccitto said that the tool provides information about services, including food, showers, toilets and appropriate rest facilities, including trading hours for service centres.

He said this tool will allow drivers to go online and see which facilities are still operational and providing these important services, thus allowing them to plan routes and breaks.

The map can be accesses at https://nhvr.maps.arcgis.com/apps/webappviewer/index.html?id=eb63f81247844052aaad2f71fe31792c.

COVID-19: Federal Government Underwrites Domestic Aviation Network

---

Adapted from media release, The Hon Michael McCormack MP, Deputy Prime Minister and Minister for Infrastructure, Transport and Regional Development, 16 April 2020

Deputy Prime Minister and Minister for Infrastructure, Transport and Regional Development, Michael McCormack, has announced that Qantas and Virgin Australia Groups will operate a minimum domestic network servicing the most critical metropolitan and regional routes in Australia.

This follows on from a commitment from the Federal Government to provide initial $165 million.

Mr McCormack said underwriting the cost of the network, which includes all state and territory capital cities and major regional centres such as Albury, Alice Springs, Coffs Harbour, Dubbo, Kalgoorlie, Mildura, Port Lincoln, Rockhampton, Tamworth, Townsville and Wagga Wagga.

He said sustaining Australia's aviation industry is critical for many reasons, including supporting the movement of essential freight such as critical medicine and personal protective equipment.

Mr McCormack said this announcement complements earlier actions including underwriting international air freight and the Regional Airlines Network Support program to assist smaller regional airlines.

He said these arrangements will last for an initial eight weeks with a review mechanism in place, where the Government will continue to monitor the market and determine if further action is required.

COVID-19: Advice from the Australian Cyber Security Centre

The Australian Cyber Security Centre has issued guidance which outlines key cyber security practices for people who are working from home.

It says working from home has specific cyber security risks, including targeted cybercrime.

The ACSC has provided a number of cyber security tips to protect your work and your household's cyber security. They are:

- Beware of scams:
    - Exercise critical thinking and vigilance when you receive phone calls, messages and emails.
    - Exercise caution in opening messages, attachments, or clicking on links from unknown senders.
    - Be wary of any requests for personal details, passwords or bank details, particularly if the message conveys a sense of urgency.
    - If in any doubt of the communicator's identity, delay any immediate action. Re-establish communication later using contact methods that you have sourced yourself.

- Use strong and unique passphrases:
    - Strong passphrases are your first line of defence. Enable a strong and unique passphrase on portable devices such as laptops, mobile phones and tablets.
    - Use a different passphrase for each website and app, particularly those that store your credit card details or personal information. To use the same username (such as an email address) and passphrase for multiple accounts means that if one is compromised, they are all at risk.

- Implement multi-factor authentication:
    - Multi-factor authentication is one of the most effective controls you can implement to prevent unauthorised access to computers, applications and online services. Using multiple layers of authentication makes it much harder to access your systems. Criminals might manage to steal one type of proof of identity (for example, your PIN) but it is very difficult to steal the correct combination of several proofs for any given account.
    - If your device supports biometric identification (such as a fingerprint scan) it provides an additional level of security, as well as a convenient way to unlock the device after you have logged in with your passphrase.

- Update your software and operating systems:
    - It is important to allow automatic updates on your devices and systems like your computers, laptops, tablets and mobile phones. Often, software updates (e.g., for operating systems and applications) are developed to address security issues. Updates also often include new security features that protect your data and device.

- Use a Virtual Private Network (VPN):
    - VPN connections are a popular method to connect portable devices to a work network. VPNs secure your web browsing and remote network access.

- Use trusted Wi-Fi:
    - Using free wireless internet may be tempting; it can also put your information at risk. Free Wi-Fi by its very nature is insecure and can expose your browsing activity to cybercriminals.

Cybercriminals have also been known to set up rogue Wi-Fi hotspots with names that look legitimate and can intercept communications, steal your banking credentials, account passwords, and other valuable information.
    - Use known trusted connections when working from home, such as your home internet or mobile internet service from your telecommunications provider.

- Secure your devices when not in use:
    - It's much easier to access your information if other people have access to your devices. Do not leave your device unattended and lock your computer when not in use, even if it's only for a short period of time.
    - You should also carefully consider who has access to your devices. Don't lend laptops to children or other members of the household using your work profile or account. They could unintentionally share or delete important information or introduce malicious software to your device.
    - If you do share your computers or devices with family or your household, have separate profiles so that each person logs in with a unique username and passphrase.

- Avoid using portable storage devices:
    - When transporting work from the office or shop to home, portable storage devices like USB drives and cards are easily misplaced and, if access isn't properly controlled, can harm your computer systems with malware.
    - If possible, transfer files in more secure ways, such as your organisation's cloud storage or collaboration solutions. When using USBs and external drives, make sure they are protected with encryption and passphrases.

- Use trusted sources for information:
    - Cybercriminals and other malicious actors use popular and trending topics such as COVID-19 to spread disinformation or scam people. Impersonating, cloning or creating websites to look genuine is one way to do this (see 'Beware of scams' above). Producing and sharing false information on social media is another.
    - Be sure to only use trusted and verified information from government and research institution's websites. Think critically about the sources of information that you use and balance all evidence before believing what people share.

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).

Further details are available at https://www.cyber.gov.au/advice/covid-19-cyber-security-tips-when-working-home

---

COVID-19: "Know the Signs" of Domestic and Family Violence

The risk of domestic and family violence has increased due to lockdowns caused by COVID-19.

Women's Community Shelters has published a "Know the Signs" poster to raise awareness of the need to know the signs of somebody experiencing domestic and family violence.

Further information is available from https://mcusercontent.com/78d4c71dbee440dc484e76c72/files/ab3f891b-156d-4579-9b5e-c28d1e408c3b/WCS_Know_the_Signs_V3.pdf, or from the Women's Community Shelters website, www.womenscommunityshelters.org.au.

Important telephone numbers:

- The NSW Domestic Violence Line, tel: 1800 656463.
- 1800 Respect; National Sexual Assault Domestic Family Violence Counselling Service, tel: 1800 737732.
- NSW Link2Home Crisis Accommodation and Home Referrals, tel: 1800 152152.