



Speech By  
**Hon. Leanne Enoch**


**MEMBER FOR ALGESTER**

---

Record of Proceedings, 10 November 2022

**MINISTERIAL STATEMENT**

**Cybersecurity**

 **Hon. LM ENOCH** (Algester—ALP) (Minister for Communities and Housing, Minister for Digital Economy and Minister for the Arts) (9.54 am): All organisations, whether public or private, are at increasing risk of cybersecurity threats. Every year the speed, scale and impact of cybersecurity attacks are increasing. The sources of these cyberthreats are varied and include nation states, foreign actors and financially motivated criminal groups. The latest academic estimate of the financial impact on the Australian economy of cybercrime is \$42 billion. As reported by the Australian Signals Directorate, cybercrime is surging and, whilst federal government agencies continue to be a favoured target for cyber attacks, local and state entities are not immune. The Palaszczuk government understands this and is responding to the real and escalating threat to the data we hold and for the services we provide to Queenslanders.

Since 2016 the Palaszczuk government has invested over \$41 million in a specialised whole-of-government Cyber Security Unit within the Department of Communities, Housing and Digital Economy to provide policy and technical expertise support to enhance the resilience to cyberthreats across Queensland government agencies. Whilst each agency is responsible for the management of its ICT programs and its resilience to cyber attacks and services, the Cyber Security Unit within my department can support these efforts. The Palaszczuk government is working hard to help protect Queenslanders' data. For example, the Minister for Transport and Main Roads has announced that Queensland driver's licences will now have a two-factor verification system. We have fast-tracked this work to give Queenslanders extra protection.

Whilst government agencies are working hard in this space, personal responsibility is also critical. Unfortunately, data breaches like the ones we have seen at Optus and Medibank have far-reaching implications, and all organisations must strive to better protect the data they hold on behalf of the community. The Australian information and privacy commissioner has advised that people should be wary of scammers who are impersonating Optus, Medibank or other government organisations. The developments over the last few days with Medibank customers' data being released by criminal hackers means that everyone needs to be extra vigilant for scammers. Everyone should be taking steps to protect themselves online, so secure your devices and accounts and monitor for unusual activity. Update your devices to protect important information and enable multifactor authentication for all accounts. Phishing emails, texts and phone calls are on the rise, so do not open emails or click on links in text messages if it just does not look right. Everyone needs to be cyberaware.