Media Release

Date:	**21/7/2016**	Contact:	**Detective Sgt Gen Hickman**	Phone:	**61732781**

BUSINESS ALERT – PBX SYSTEM

Tasmania Police advice that a number of businesses from around Hobart have had their PBX (Private Branch Exchange) system compromised in the last few weeks. The PBX is a system that allows and controls the sharing of phone lines between telephones and other communication devices.

The intrusion into the business phone systems have occurred at night or over the weekends.

At least two northern suburbs businesses have had their phone system compromised:

1. The first had their phones used 673 times between 11.04pm on 8 July 2016 and 8.55am the next day. The cost of those calls was over $9,000. International calls were placed to a number of lines in Nauru, Monaco and Eritrea;

2. The second had their phones used during the weekend of 16-17 July 2016. Early estimates are that the cost will be in the vicinity of $5,000.

The cybercriminals target the phone system and usually gain access through an insecure or weak password. They then use the outbound call feature to forward calls to a 'phantom' mail box that will give a dial tone. This allows them to make international phone calls at the businesses' expense. Those calls may be to numbers actually owned by the hackers and are charged at a premium rate.

Costs associated with this fraud may be borne by the affected company.

There are prevention strategies:

1. Ensure your passwords are not on factory settings. If able, choose complex, random passwords of at least six to eight digits. Don't use obvious passwords such as address, birth date, phone number, or repeating, successive or ascending numbers, i.e. 000000, 123456.
2. Don't use any unsecure features. Voicemails are a vulnerable common feature of Australian PBX systems. Disable features such as international call forwarding or external transferring of calls to decrease the risk of a hacker using this type of access to manipulate your PABX. If these features are not required by your employees, turn them off.
3. Consider disabling the remote access or limit it to employees that have a real need for such a feature.
4. If your system permits, do not allow unlimited unsuccessful attempts to enter voicemail, three attempts should be sufficient and should default to call failure.
5. Speak to your phone system provider about other ways to protect your system from hackers.

If your system has been hacked:

1. Engage with your phone system provider to identify the intrusion point and take all protective action you are advised of.