

June 2011

PABX FRAUD ALERT – PABX HACKING

There has been a recent increase in the fraudulent hacking activity hitting many businesses with a PABX, involving international calling. Much of this activity relates to a practice known as “International Revenue Share Fraud” (IRSF).

IRSF is a form of traffic inflation or flooding whereby an international revenue share provider obtains a number, or range of numbers designated as a premium rate service (PRS) which allow callers to access some form of entertainment service/feature, such as mobile ringtones, screensavers, horoscope readings etc, usually 190X numbers in Australia and more notoriously 900 numbers in the US.

Each call to a PRS generates profit for both the revenue share provider and the content provider, ranging anywhere between 30% and 80% of the net tariff. Fraudsters have been known to enter into arrangements with the PRS content providers, with the purpose of flooding traffic to them using various methods, most commonly via hacking PABX, VoIP or Voicemail and programming the extension to automatically dial the PRS number.

Look for the signs!

You should consult with your PABX maintainer to determine if your system may have been a target.

Here are some possible warning signs:

- While retrieving voicemail the system returns a 'busy' error message.
- Heavy call volumes late at night on weekends and public holidays.
- International calls on your bill to places you don't usually call.
- Calls of very short duration on your bill ie. calls under ten seconds.

How To Protect Your Business:

How you protect your business is a matter for you to determine in consultation with your PABX maintainer.

Here are just some of the ways that you can protect your system:

- Regularly change your voicemail pins and do not use default pins such as 1234.
- Disable any call forwarding or outbound call ability from your voicemail ports.
- Cancel any unused voicemail boxes.
- Block all International calls access unless absolutely necessary.
- Block International call access to countries that you don't usually dial.
- Ensure your PABX admin access unit is kept in a secure location.
- Restrict the 'after hours' outgoing call access.
- Disable DISA access unless absolutely necessary.
- Look for heavy call volumes at night, on weekends and public holidays.
- Review system call records for discrepancies and unusual use.

Due to the ability of carrier override codes (eg. 0018 – Telstra Easy Half Hour, 0019 – Optus International Fax line) hackers can even determine which company bills you. Therefore you may receive a bill from a phone provider you are not currently a customer of.

Please note that the legal liability for the traffic and payment for international charges rests with the customer under the terms and conditions of our agreement, so it is important that you remain vigilant regarding your PABX security.

If you have concerns or require further information please do not hesitate to contact me.

Kind regards
Cherry Sawyer
Complaint Resolution Manager