

PABX Fraud...Can Cost your Business \$\$

Hacking of PABX systems causes substantial losses to Australian Companies each year. The PABX features which businesses are wanting for their phones, can in fact pose significant security risk.

Who is Responsible?

PABX fraud can cause unauthorised call charges on your telecommunications accounts. The amounts can easily run into \$1,000's over a weekend.

As a business owner you are responsible for maintaining the integrity and security of your company's phone system. However you may not even be aware that such a risk exists this does not negate the responsibility you will have for any call charges that may originate from your system. As each system is different it is important that you contact your PABX maintainer for any advice they may have to prevent such risks.

If Trinity Telecom becomes aware of possible PABX fraud it may provide a notification to you as a courtesy but this can only occur *after* the fraud has commenced. Trinity Telecom is not responsible for the security maintenance of your company phone system and will not be held responsible if it does in fact become compromised. You as the customer will be required to pay any and all charges generated as a result of any fraudulent behavior.

How Does it Happen?

Computer hackers remotely access a company's PABX system to make long distance and overseas phone calls. The calls are most often to obscure international destinations for their own personal financial gain. The costs are borne by the business that owns the PABX that has been hacked as the calls come through as per normal and are charged on your normal bill, the amounts can be quite substantial.

Hackers exploit weaknesses in PABX system's by figuring out voicemail PIN's and gaining access via the PABX maintenance port or 'Direct Inward System Access' (DISA) point of the PABX. Once they gain access to the voicemail they are then able to remotely re-program a PABX system and make International telephone calls whenever they like or via automated services.

The hackers may even re-sell the calls as a phone operator themselves or even worse they may even divert the calls to their own overseas premium rate phone services racking up huge call charges. Both of these create income for the hacker, while the business who has had their PABX hacked is left with the bill. Due to the large numbers of lines that many PABX systems have, the cost to the business can escalate very quickly and without notice over weekends or holidays as many calls can occur simultaneously. If a bill cycle is some weeks away the costs can easily become astronomical and go completely unnoticed.

Protecting your business from Hackers

This is a matter for you to determine in consultation with your PABX supplier or maintainer.

Here are just some suggestions that may assist in protecting your system:

- Regularly change the PIN's on your voicemail services
- Don't use default PIN's such as 1234

- Disable any call forwarding or the ability to make outbound calls from your voicemail ports
- Cancel any unused voicemail boxes
- Bar International calls access unless absolutely necessary at your PABX and also with Trinity Telecom
- Bar International call access to countries that you don't normally dial
- Ensure your PABX administration access unit is kept in a secure location
- Restrict the 'after hours' outgoing call access
- Disable DISA access unless absolutely necessary
- Enable your online bill with Trinity Telecom and check on your unbilled calls periodically
- Look for heavy call volumes at nights or on weekends and public holidays

What Signs can I look out for?

Consult with your PABX maintainer to see if your system has been a target.

Here are some possible warning signs.

- When retrieving voicemails your system returns a 'busy' error message
- High call volumes late at nights or on weekends and public holidays
- International calls on your bill to countries you don't usually call
- Calls of very short duration on your bill i.e. calls under ten seconds.

PABX Fraud can have a serious impact on your business:

Case Study 1:

An Australian bank was the victim of PABX Fraud. Hackers had accessed the company's system through the company's main switchboard and jammed the phone to constantly dial a number in Sierra Leone. The following business day, the staff noticed that their voicemail boxes were constantly busy and thought that there may have been an IT problem but didn't think to alert their maintainer. Their carrier noticed the breach several days later and notified the customer that approximately \$10,000 worth of calls to Sierra Leone had been run up in a period of only 6 days.

Case Study 2:

A government department was a recent victim of PABX hacking. Their carrier noticed the unusual call traffic and alerted the customer within 24 hours of the fraud occurring. Due to problems with finding the correct person to handle the issue, the problem was not rectified for approximately 14 days after the initial breach. The customer eventually received their bill to find out that \$80,000 worth of calls to Columbia occurred as a result. The customer was liable to pay the charges.

Case Study 3:

A small business suffered a recent PABX attack. The business was a customer of Trinity Telecom and was notified the day before Christmas of unusual phone calls to international destinations. The customer was notified but was on holidays was not concerned and did not notify their PABX maintainer. Over the Christmas break further breaches occurred and a bill of over \$6000 was generated.

Please contact Trinity Telecom if you wish to bar or restrict International calls on 1300 786 192