



Modcoms Voice Data Mobility Guide to Minimizing Toll Fraud

Important information on how you can better protect your business against unauthorized PABX access.

What is Toll Fraud?

PABX Fraud, also known as Toll Fraud, causes multi-million dollar losses to organisations each year. This is now beginning to have a substantial impact on business' in Australia.

Toll Fraud is the fraudulent use of an organisation's telephone lines to enable fraudsters to make long distance telephone calls at little or no cost to themselves. However, the cost to the organisations affected can be considerable.

This fraudulent action inevitably results in very large telephone bills and costs through security breaches for the company that was hacked.

Who Pays The Bill?

As a company, you are responsible for maintaining the security of your phone system. In some instances, your carrier may alert their customers to possible PABX security breaches, but it is not responsible for the security maintenance on your system. Likewise, Modcoms Voice Data Mobility is limited to advising you of the possible threat and ways in which you can better protect your particular telephony solution.

No responsibility will be taken by Modcoms Voice Data Mobility should your PABX system become compromised. At the end of the day you will be required to pay any charges generated as a result should you carrier insist on payment



POTENTIAL WAYS THEY CAN DO IT?

Hackers fraudulently use a company's PABX system to make long distance telephone calls, usually to obscure international destinations at no cost to themselves. The costs are charged to your organisation and can be quite considerable.

The more sophisticated PABX systems become, so do the hackers and their software. Hackers exploit weaknesses in the company's PABX system by figuring out voicemail pass codes and gaining access via the 'Direct Inward System Access' (DISA) point of the PABX. Once they penetrate the voicemail they are then able to make international calls.

The fraudsters will often then either on-sell the calls as a phone operator themselves or they may even divert the calls to their own premium rate services. Both methods derive income for the hacker, while the business is left with the bill. Due to the unlimited numbers of lines that most PABX systems have, the cost to the business can escalate rapidly as many calls can occur during any one time. The hacker will often breach the system late at night when the business is not operating so they can attempt to avoid detection.

HOW TO PROTECT YOUR BUSINESS

Educate your staff

- Brief your staff on security procedures and the importance of following them;
- Establish procedures for staff to report any suspected security breaches immediately.

Passwords/Codes

- Use random numbers for PIN's on the Telephone System or voice mail box, which should utilize the maximum number of permissible digits;
- Ensure system passwords and codes are not left as default, particularly system administration passwords;



- Cancel extensions (or at least check any forwarding and remove STD/IDD access), passwords and security codes of departing employees;
- Change passwords and security codes as often as possible;
- Do not divulge passwords/codes or modem access numbers over the phone;
- Limit the number of staff who have administration access to your system, and change passwords if there is any turnover of staff;
- Only allow one, or a small number of reputable “service providers” to work on your system, and satisfy yourself that they understand ‘fraud’ risks;
- Ensure that people responsible for performing moves and changes on your system, have guidelines as to what authority is required before making changes which may expose your system to fraud (e.g. granting IDD access).
- Do not use PIN’s such as 0000, 1111, 1234, 4321, 9999. These are the first passwords to be used by a fraudster.

Trunk Access (Outgoing Call Access)

- Bar access to countries or interstate locations that do not require telephone access, if you do not do business in that area there is no necessity to make calls there;
- Do not allow Voice Mail, Interactive Voice Recognition (IVR) or other such systems to have outgoing trunk access or external call forwarding unless absolutely required;
- Do not allow Voice Mail Systems to have international trunk access without serious consideration;
- If possible, disable the ability to forward extensions to outside lines (e.g. ‘0’), trunks and/or just IDD numbers;
- When extensions are moved through software, ensure that any special access rights (e.g. IDD access, call forwarding) are removed from the ‘freed’ port;
- Ensure effective call barring has been carried out;
- “Night Switch” the system to stop all outgoing calls after hours (except emergency 000) where possible and ensure the authorized night switching station is in a secure location.



Ways in which Modcoms Voice Data Mobility can assist to increase the security of your telephone system:

- Disable any call forwarding or outbound call ability from your voicemail ports
- Cancel any unused voicemail boxes
- Update the pass code for voicemail administration access
- Restrict the 'after hours' outgoing call access
- Disable DISA access unless absolutely necessary

WHAT TO DO NEXT

We suggest you begin by following the steps to protect your business as outlined above. If you would like to enlist the assistance of a telephone technician to consult with you on further securing your PABX please email our Service Department on service@modcoms.net.au