

Toll Fraud Minimisation Guide

A practical guide for Commander Customers to reduce the risks associated with the phenomenon of Toll Fraud on Telephone Systems

Introduction

Toll Fraud causes a multi-billion dollar loss worldwide each year and is now beginning to have a substantial impact in Australia. Toll Fraud is the fraudulent use of an organisation's telephone lines to enable thieves to make long distance telephone calls at little or no cost to themselves. However, the cost to the organisations affected can be considerable.

Hackers or Fraudsters illegitimately access telephone systems for many reasons, but the primary reasons are to obtain free calls (often for on-sale), steal company information or cause malicious damage. This inevitably results in very large telephone bills and costs through security breaches for the company that was hacked.

This document explores the motivations fraudsters have for committing toll fraud offences and more importantly outlines some basic steps Commander customers can take to reduce their risk and exposure to Toll Fraud incidents.

Why is hacking becoming a problem in Australia?

Hacking has not yet become as widespread a problem in Australia as it is in other worldwide regions. However there have been some recent incidents and the frequency of these incidents is liable to increase for the following reasons:

- The sophistication of telephone systems available to companies in Australia is increasing;
- Services operating over IP networks or the Internet provides methods to access Telephone Systems;
- ACMA (Australian Communications and Media Authority) allow many features on PABX's such as Trunk to Trunk connections to be used;
- Wide use of maintenance modems and remote access via the Internet on telephone systems;
- Voice Mail and Unified Communications Systems that allow outbound calling capabilities;
- Widespread use of the Internet which to posting information exposing system vulnerabilities and sometimes specific system access information;
- The huge demand for free international calls as overseas nations develop their telephone networks and business requirements;
- Customers either ignoring, or more likely, not being aware of the hacking problem thereby leaving their telephone systems open to abuse;
- Direct Inward System Access (DISA)

What can be done to prevent the telephone system from being hacked?

The principal factors that attract a hacker to a telephone system include:

- Freecall numbers connected to the telephone system;
- Remote Access to the telephone system (Via modem or Internet) if not implemented securely;
- Voice Mail Systems (particularly if through-dialling is enabled);
- Systems with a large number of trunks / DDI trunks;
- Direct Inward System Access (DISA);
- Default Passwords;
- Ability to forward phones to external numbers
- Wide access to STD and IDD dialling.

Hacking counter measures

The primary method of preventing fraudulent access to the telephone system is for the customer to educate its staff with regard to telephone security. Implementing all, or at least some, of the following simple steps can reduce the susceptibility of a system to being hacked.

What can you do?

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;
- Do not allow your Internet gateway to be remotely accessible from the Internet (particularly on standard ports) and if you need it remotely accessible, ensure secure username and password selection.

Passwords/Codes

- Use random numbers for PINs on the Telephone System or voice mailbox, which should utilise 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 nor write them in Email;
- Ensure that the Network Service Provider is aware of the "normal" traffic levels on the system and discuss with them notification of "sudden" or "dramatic" increases in traffic volume;
- Consider changing remote access details from time to time (eg. Modem numbers). Always advise your service provider of any changes as often remote access to the PABX modem is the fastest way to resolve service difficulties;
- Block remote access via the Internet unless specifically required at the time remote support is necessary. Any access from the Internet should be secured and not via standard TCP ports;
- 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).

Trunk Access

- Educate everyone not to connect anyone they do not know to an outgoing trunk;
- 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, Auto Attendant (AA), 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 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 authorised night switching station is in a secure location.

Monitoring the telephone systems

- Familiarise yourself with calling patterns and review them regularly. Look for any afterhours call activity;
- Study Call Detail records and billing records for any signs of fraudulent activity
- Review Voicemail reports;
- Look for heavy call volumes at nights or on weekends and public holidays;
- Have your telephone system audited (by yourself or your supplier) at regular intervals to check for security weak points and how well the programming suits the needs of the Company. Investigate the features of newer releases with your supplier.

System Information

Guard information on the Telephone system:

- Network service provider's authorisation codes should be kept in a secure location;
- Do not write authorisation codes and passwords in notebooks;
- Don't throw out call detail records and system information. Criminals often sift through the rubbish to obtain information. Dispose of these records using secure methods (Shredding or Security bins);
- Keep all System Manuals in a secure location and do not write information that may be useful to hackers in these manuals. Cabinets used to store system manuals should be kept locked;
- Customers and technicians should dispose of sensitive information securely and not leave information useful to hackers in the PABX room.

Equipment Room Access

- Access to the telephone system should be restricted as much as possible;
- Customers should ask for identification before allowing access to the telephone system (Including remotely);
- Where possible, the telephone system and peripherals should be kept in a secured location such as in a locked communications / server room (with adequate ventilation).