commander

BE SECURITY SMART

Follow these best practices to protect yourself and your business from fraudulent attacks.

COMM_CO3_0001_01/19

EDUCATION

- Brief your staff on security procedures and the importance of following them;
- Establish procedures for staff to report any suspected security breaches immediately;
- Educate all staff not to connect anyone they do not know to an outgoing trunk.

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;
- Change passwords and security codes as often as possible;
- Do not divulge passwords/codes or modem access numbers over the phone or write them in email;
- 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;
- Limit the number of staff who have administration access to your system, and,
- change passwords if there is any turnover of staff.

SECURE YOUR SYSTEM

- 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 reason to make calls there;
- Do not allow Voice Mail, Auto Attendant (AA), Interactive Voice Recognition (IVR) or other 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;
- Where possible, disable the ability to forward extensions to long distance and/or international numbers;
- When extensions are moved through software, ensure that any special access rights (e.g. international access, call forwarding) are removed from the 'freed' port;
- Cancel extensions (or at least check any forwarding and remove long distance and international access), passwords and security codes of departing employees; and,
- Ensure effective call barring has been carried out.

"Toll fraud can enable thieves to make costly calls at your expense - but it is simpler than you think to keep your business safe from fraudulent attacks."

AND IF YOU RUN A PABX

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; and,

Only allow one, or a small number of reputable "service providers" to work on your system, and satisfy yourself that they understand 'fraud' risks.

SYSTEM INFORMATION

Always guard information on your Telephone system:

- Network service provider's authorisation codes should be kept in a secure location;
- Do not write authorisation codes and passwords in notebooks;
- Do not 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.
- Ensure that people responsible for performing moves and changes on your system have clear guidelines around what authority is required before making changes which may expose your system to fraud (e.g. granting IDD access, opening remote access or changing passwords).