IT'S HOW WE CONNECT

PROTECTING YOUR PABX, VoIP or VOICEMAIL- Q & A

WHAT IS PABX?

Private Automated Branch Exchange (PABX) is a system that allows and controls the sharing of phone lines between telephones and other communication devices.

WHAT IS PABX HACKING?

PABX hacking is more commonly referred to as 'toll fraud'. PABX hacking occurs when fraudsters search for and detect vulnerable access points in a PABX system. It is a damaging act of Customer Premise Equipment (CPE) fraud that impacts Australian businesses and companies worldwide. The impact sustained by victims of PABX fraud is not only associated with monetary losses but it can also cause reputational damage.

WHO ARE PABX HACKERS?

PABX hackers are fraudsters who gain unauthorised access to your PABX, voicemail, VoIP or other communications systems. Hackers can be disgruntled employees or ex-employees, local or international hackers, call selling operations or organised crime networks

WHY DO THEY DO IT?

Toll fraud can be a lucrative business for a hacker, who can compromise an unprotected PABX system by dialling in remotely with the intent to use for fraudulent means. Hackers can be motivated to commit PABX fraud by the thrill of the act, the notoriety gained, the challenge, or from the potential money they can make. The intention of PABX hackers is to damage the reputation of your business by overwhelming your phone lines with rogue calls at no cost to them, often to overseas numbers and at premium rate services. Your business is not alone. **ALL** companies that operate a PABX are at risk.

IS YOUR PABX PHONE SYSTEM SECURE?

Most PABX systems have standard security settings in place. It is important to understand the parameters of the security settings and work with your PABX maintainer so that basic countermeasures are implemented to minimise the risk of an external hack.

HOW CAN YOU MAXIMISE THE PROTECTION OF YOUR PABX?

- **Make sure your login is secure.** Verify with your system maintainer that all factory default passwords and pin numbers have been changed. Avoid using weak pass codes such as 0000, 1234 or the last 4 digits of your phone extension. Change your password on a regular basis, such as every 30 days.
- **Don't use unsecure features.** Voicemails are a vulnerable common feature of Australian PABXs. Disable features such as international call forwarding or external transferring of calls to decrease the risk of a hacker using this type of access to manipulate your PABX. If these features are not required by your employees, turn them off!
- **Disable remote access.** Features such as Direct Inward System Access (DISA) are used by technicians, engineers or contractors whereby they can connect via modem and log in to your PABX to perform changes and upgrades remotely. If you have VOIP or internet connectivity, use firewall rules to block all undesirable internet activity and close unused IP ports. Limit the access to current and authorised personnel or employees only. Disable these access ports immediately once they are no longer required. Ensure that your maintainer or any party requiring external access obtains verbal confirmation prior to any work being carried out on your PABX.