

We take customer's security as top priority, ensures customer details are stored in secure environments, and password protected to prevent anybody not authorised to obtain details about our customers, from accessing any of this information.

Additionally, we provide information about reducing your risk to Telecom Hacking and Toll Fraud.

We recommend that you protect against unauthorised access to or use of your services by:

- Regularly monitoring your usage to check for irregular patterns;
- Protecting your user identity, email address and passwords;
- Exercising care in disclosing personal information on the internet;
- Using current anti-virus software and firewall;
- Restricting access to your equipment;
- Being careful if accepting emails or files from unknown sources.

## Toll Fraud Notice

---

### **Your phone system may be vulnerable to toll fraud**

Your business could be a potential target of PABX Hacking or Toll Fraud. Unless you have taken steps to secure your system, hackers may be able to gain access to your phone system and make calls to Local, National, Mobile and International numbers. Access is often gained through voice mailboxes with weak passwords. Once inside your system hackers can use system commands to make calls that could result in phone charges amounting to thousands of dollars.

Access is sometimes gained via factory default passwords that were not changed when the phone system was installed. You should confirm with your maintainer that your phone system's security features have been enabled to provide maximum protection, as you are liable for charges for all calls made through your phone system.

Should you wish to know more about the risks associated with PABX hacking, please call your Phone System Maintainer or our Customer Care Team.