Security Tools

Account Security Tools

bVivid customer accounts are protected by password. The initial password at account opening is created by us and should be changed by you as soon as possible. Weak passwords will be automatically detected by the system when a customer attempts to log in and a warning will pop up to increase the strength of the password.

A strong password is one that is a minimum of 8 characters has a mix of upper and lower case letters, numbers, special characters (!@#$ etc.) and is not substituting numbers or special characters for the letters of a dictionary word or name.

Password Reminder

bVivid has an automated password reminder system if you have forgotten your account password. This can be requested by calling 1300 833 177 and following the prompts to customer service.

Customer Account ID Verification

Before we can access and discuss your customer account, you will be asked to provide certain identity information we have previously collected from you, most typically at account opening. You can nominate Authorised Representatives to act on your behalf and once a representative has been set up, the identification process applies to them as well when they call on your behalf. Call 1300 833 177 if you have any questions in relation to our account security measures.

Security Tools

We take our Customer's security seriously, and the security of our customer details is stored in secure environments and is password controlled to protect from someone not authorised to gain information about our Customers. Additionally, we provide information about reducing your risk to Telecom Hacking, Toll Fraud.

We recommend 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;
- be careful if accepting emails or files from unknown sources.

Toll Fraud Notice

Is your phone system 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 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.