

We have recently seen an increase in the instances of PBX Fraud/Phone Hacking. Phone hacking is fraud that normally arises through unauthorised access to “dial through” functions on a telephone system that does not have sufficient security measures in place.

The purpose of this guide is intended to make you aware of the potential risk, the steps you can take to reduce the risk and stop unauthorised third parties from accessing your telephone system to make calls (usually to overseas destinations or to premium rate numbers).

You are responsible for payment of all costs relating to telephone calls made from your phone system. This can have a serious cost implication for business so it makes sense to make your phone system as secure as your data network.

### **What measures can be taken to protect your business?**

There are a number of measures that can be taken to ensure that your telephone system is better protected:

1. Contact your system maintainer to ensure voicemail and remote access is secured, and if external access is not required to disable the functionality. Your system maintainer can also advise on other security functions of your telephone system.
2. Ensure that the number of personnel that have remote access to your system is restricted and that each individual has a different access code. If an individual leaves the company, then ensure their access code is disabled immediately.
3. Never use common default access codes for systems; ensure that they are changed after installation. Ensure the access code uses the maximum number of digits that the system allows. Change the access codes regularly, choosing random numbers so that a pattern cannot be found.
4. Treat all information related to the access codes as top level security. Store the information securely and only give staff access to it on a need to know basis. Those members of the team that do have access to the information should be aware of its importance and the risks involved if they divulge it.
5. Never use a telephone number or extension as an access code as this will make it easier to decipher the code.
6. Where possible always use call barring or other restriction codes. Give high priority to monitoring the system activity to check that no hacking is taking place. Call barring can be placed on your telephone system or at the network level.
7. Set up your company email alerts at [www.swainstel.info](http://www.swainstel.info). This service will not prevent the fraud but it will alert you to unusual activity such as out of hours calls, or calls over a specific duration/cost, usually with 1 working day of the activity. You can also use this site to download your invoices, check traffic and more. If you require a new password please contact Swains Plc on 0844 257 2800.

Please contact your System Maintainer if you need further advice or assistance in protecting your business from PBX fraud.