How to protect your business: Anti-Phreaking

There are some simple security guidelines to follow:

- Always change the default password from the one provided by the voice mail vendor at the time of voice mailbox initialization.
- Change your voice mail password frequently. Eliminate the advertising or publication of default passwords.
- Don't use obvious passwords such as a birthday, phone number, or successive numbers, i.e.123456. Do not use sequential, ascending or descending numbers or any part of the telephone number for your passwords.
- Check your recorded announcement regularly to ensure the greeting is indeed yours. Hackers tend to attack voice mailboxes at the start of weekends or holidays.
- Consider blocking international calls if possible on your phone system.
- Consider disabling the remote notification, auto-attendant, call-forwarding and out-paging capabilities from voice mail, if these features are not used.

How will I know if hackers are/ have been in my Voice Mail System?

- You may notice lights on phone lines that are lit up without anyone using the phone.
- You get an alert from your Long Distance and/or Local Telephone Company stating that there is suspicious activity on your phone lines.
- You receive a bill for international calls that are made from one or more of your lines that were not dialed by anyone in your company.

How can I prevent phone fraud?

The simplest way is to upgrade your phone system to a level that has a PABX firewall built-in, or select a single add-on that will protect your organisation.

For further support or more information on add-ins or upgrades please contact Amillan on
0845 504 8885

What is 'phreaking' or voicemail fraud?

A hacker calls into a voice mail system and searches for voice mailboxes that still have the default passwords active or have passwords with easy sequence combinations i.e., 123456. The hacker then uses the password to access the phone system and places domestic or international calls. Sometimes, the hacker even establishes new mailboxes on the system.

Hackers gain entry to the system by various means. Some hackers call in on toll free lines intended for customer use. Some use stolen calling cards. Some will even pretend to be someone they are not to socially engineer their way into your system.

Once in your system, the hacker may break into voice mailboxes which have remote notification activated and then forward calls or messages to the mailbox owner. They change the remote notification service to forward to a domestic or international number. They are then able to make a domestic or international call at your expense.