TELEPHONE SECURITY CHECKLIST

Your telecoms provider is a member of the FCS, a trade association which promotes best practice in communication services. They have given you this checklist to help you secure your phone system against fraudulent use. It is not a guarantee of security but you are advised to carry out the steps below to help protect your company. For further information about cyber security, visit https://www.cyberstreetwise.com/

INSTALLER CHECKLIST (to be completed by your provider before hand-over)

- Follow manufacturer's advice to utilise maximum security settings
- Set a secure system password of at least 6 digits with stars if possible
- Set system to block all stations from dialling 09, 118 and international numbers (including 123)
- Change all authorisation passwords to be secure – at least 4 digits
- Turn off any feature that allows auto-create of new extensions
- Include a session border controller for SIP firewall
- Change default passwords in all administrative areas
- Enable authentication option for SIP trunk access
- Limit the incoming SIP dialling plan to prevent SIP destination modification
- Block remote access/outbound calls via voicemail ports
- Block out of hours calls

Before leaving site:

- Give customer this checklist
- Inform them of system password (unless CP is maintaining control of system)
- Inform them remote voicemail access is "off"
- Inform them of limited out dial destinations
- Obtain customer signature showing acceptance of set-up and checklist.

FIREWALLS CHECKLIST (make sure your IT department receives this checklist)

Dynamic IP addresses:

Enable authentication for all user accounts with robust passwords

Connections to Trunk/Interconnect Providers:

Configure firewall to allow only authorised interconnect traffic to and from the provider.

Restrict Media Port Range:

Set a range appropriate for the expected maximum number of concurrent calls

Protect management interfaces:

Configure firewall to allow access to management interfaces only from authorised IP addresses

CUSTOMER CHECK LIST (a senior manager should be aware of these safeguards and ensure staff follow them as relevant)

- Remove all default password settings when deploying the PBX and limit access to any maintenance ports.
- Passwords and access codes should be changed regularly and if possible be alpha/ numeric and as many digits as the system allows. Avoid 000, 1234, extension number=PIN passwords
- Delete/change passwords for ex employees
- Consider limiting call types by extension, if an extension user has no requirement to ring international/premium rate numbers then bar access to these call types.
- DISA - (Direct Inwards System Access) is typically used to allow employees to dial in from home and make outbound calls (usually high value call types, ie mobile, international etc) via the company PABX. Your CP has deactivated this; if reactivated it should be closely controlled.
- Secure the system physically, site it in a secure comms room and restrict access to that area
- Regular reviews of calls should be carried out to cover analysis of billed calls by originating extension also to identify irregular usage and unexpected traffic
- Ensure you fully understand your system's functionality and capabilities and restrict access to those services which you do not use.
- Mailboxes - block access to unallocated mailboxes on the system, change the default PIN on unused mail boxes
- Be vigilant for evidence of hacking - inability to get an outbound line is usually a good indicator of high volumes of traffic through your system. Check for calls outside business hours.
- Assess security of all PBX peripherals/applications: platform, operating system, password and permissions scheme. Carefully evaluate the security of any onboard remote management utility (eg PC Anywhere) for possible holes.
- Check firewall logs weekly
- If relevant set access PIN on smartphones that will use VOIP
- Limit VOIP registrations to office network
- For SIP systems, set credit limits per phone per day