MF TELECOM SERVICES

PROTECT YOUR TELEPHONE & HOSTED SYSTEMS FROM FRAUD

Telephone and hosted system fraud is a global problem, with an average incident costing in thousands. We've put together a checklist to see how you can keep your business protected.

- Passwords and access codes should be changed regularly, alpha/numeric characters, and as many digits as the system allows
- 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
- If possible, restrict outbound calls outside working hours
- Secure the system physically in a secure comms room and restrict access to the area
- Regular review 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 systems functionality and capabilities and restrict access to those services that you do not use
- Mailboxes - block access to unallocated mailboxes on the system, change the default PIN on unused mailboxes. Remove an unused mailboxes
- 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
- Access the security of all telephone and or hosted system peripherals/applications: platform, operating system, password and permissions scheme. Carefully evaluate the security of any onboard remote management utility (e.g. PC Anywhere) for possible holes
- Check firewall logs weekly