

Call fraud is currently on the rise, and Modern encourages you to take the necessary precautions to prevent it from happening to you!

Modern already have in place a number of solutions at network and day to day operational level that are designed to both identify and react to unusual patterns.

There is a lot you can do to prevent this occurring in the first place! Prevention is better than cure!

Tips to help you guard your business from fraud

1. Remove or de-activate all unnecessary system functionality including remote access ports. If you must have the latter, protect them with strong authentication techniques such as smartcards or tokens.
2. Restrict the numbers that employees can dial: for example, bar calls to premium rate numbers, international numbers, operator numbers or Directory Enquiries.
3. Review your PBX call logging/reporting records regularly to spot any increases in call volumes or calls to suspicious destinations.
4. Bar voicemail ports for outgoing access to trunks if you can. Change your voicemail and DISA (Direct Inward System Access) passwords regularly and don't use the factory defaults or obvious combinations such as 1234 / 0000 or the extension number.
5. If access to trunks via voicemail is vital, then introduce suitable controls. Remove Auto Attendant options for accessing trunks too.
6. Lock any surplus mailboxes until you have a user for them.
7. Not using DISA? Then disable it completely.
8. Restrict access to your core comms equipment, such as your comms room or master terminals.
9. Only give individuals the appropriate and minimum level of system access they need to carry out a specific task.
10. Change your security features - passwords, PINs etc - and re-set the password defaults whenever you install, upgrade, repair or maintain equipment.
11. Treat all internal directories, call logging reports or audit logs as confidential. Destroy them securely when they're no longer needed.
12. Avoid using tones to prompt for password/PIN entry: hackers find it easy to duplicate them.
13. Implement formal processes to cover employee entry procedures, the issuing of pass cards, the vetting of new employees and when people change jobs or leave. For the latter, remember to revoke any access they might have had to your systems, mailboxes or buildings.
14. Review your system security and configuration settings regularly. Follow up any vulnerabilities or irregularities promptly.
15. Be vigilant against bogus callers: people who pose as a company employee and ask to be connected to a switchboard operator to get an outgoing line.

Please remember that you are responsible for any calls made from your premises and equipment and any cost incurred.