

Telecommunications fraud affects everyone who uses communications equipment. By having a properly secured telephone system, you can help ensure your business's continuity and mitigate potential damages to your business resulting from toll fraud. The purpose of this document is to outline the top 10 ways that your business can secure its telephone system.

Here are the top 10 ways of preventing telecommunications fraud:

1. Set up a password system to protect your business from PBX/VM Fraud. Randomly change the password that allows access to any Direct Inward System Access (DISA) port. Make sure that only those employees who really need to use this system have the password.
2. Restrict call forwarding features on your company PBX or key-system to local calls only.
3. Block calls from processing through your PBX system or Operator Center to certain high fraud areas such as Bangladesh, Cuba, Haiti, India, Pakistan, Philippines, or other areas you may identify.
4. Restrict the collect calling option on all your incoming phone lines, including voice mail lines. Ask your Account Executive to add Billed Number Screening to your telephone numbers.
5. Establish a line-monitoring system that will alert you to possible fraudulent use of your private network or PBX equipment.
6. Educate your employees, particularly those who use calling or credit cards, about safeguards to use when placing calls from public telephone facilities. "Shoulder Surfing" (visual eavesdropping) is still prevalent and employees should protect their card numbers by keeping them hidden from casual observers while using them.
7. Use calling cards that offer PIN options to each cardholder. Like a computer password, the PIN number is hidden and the call cannot go through until the PIN number is entered. Encourage employees to use something other than a date of birth, or other easy to guess numbering sequence, so that the code is more difficult to crack.
8. Educate your family, friends or employees to NEVER give their calling card numbers, or PIN numbers, to anyone who calls them. If someone calls to verify a card or PIN number, it is more than likely a scam since legitimate companies would not use this approach.
9. Arrange for all cellular users in your employ, or in your family, to have their own PIN code to protect against cellular fraud.
10. Protect your company's internal telephone directory. Restrict use to employees only. Adopt strict distribution controls and penalties for failure to comply with the privacy requirements of your company. When finished with the directories, have them shredded.

tw telecom

Network Operations Center – Fraud
888-245-0608