PBX & Voice Mail

- **Private Branch Exchange (PBX)**

  A PBX is a private switch, either automatic or manually operated, serving extensions in a business and providing access to the public network. A **DISA** (Direct Inward System Access) permits convenient access to a PBX form a phone outside the business using an 800 number or other special access number so that authorized persons can bill long distance calls to the company's PBX. The DISA gives criminals this same opportunity, as well as the chance to set up a call-sell operation at the company's expense.

More tips

- Don't allow unlimited attempts to enter your system. Program your PBX to disallow access after the third invalid access or barrier code attempt.
- Directories or business cards that list PBX access numbers should be shredded before being placed in the trash.
- Never give out technical information about your system unless you know to whom you're giving it.

200 copies of this brochure were printed at a cost of .03 ¢ per copy.

Public Utilities Commission
State Capitol Building
500 E Capitol
Pierre SD 57501
Phone: 800-332-1782
Fax: (605) 773-3809
www.state.sd.us/puc

Business Call Schemes

Public Utilities Commission
State Capitol Building
500 E Capitol
Pierre SD 57501
Phone: 800-332-1782
Fax: (605) 773-3809
www.state.sd.us/puc

More Tricks

- **Voice Mail Systems**

  Systems that provide out-dial or through-dial capability can be used fraudulently by transferring out of a system - intruders can place long distance calls. Trespassers look for default codes on mailboxes so they can change the codes and control the boxes.

- **Other Scams**

  Imposters seek out passwords, authorization numbers, and access codes by snooping around offices, calling businesses, even rummaging through dumpsters. Comprised numbers are sold or traded in the phone fraud underworld with the unsuspecting business owner picking up the resulting bill.

Protection Tips

- Be alert to overt signs of PBX abuse:
  - repeated calls of short duration,
  - unexplained increases in incoming or outgoing calls,
  - sudden increase in 800 usage,
  - change in after-hours calling patterns.
- If practical, eliminate remote access To your PBX and replace it with telephone calling cards for authorized personnel. If you eliminate remote access, make sure to disable the access system.
- Carefully examine all billing information to identify unauthorized calling patterns. Frequent review can save money.
- A delayed electronic call response can provide added security. Your PBX should be programmed to wait at least 5 rings before answering a call.
- A steady tone used as a remote access prompt leaves your system vulnerable to perpetrators' automatic dialing programs. Use a voice recording or silent prompt instead of a tone.
- Tailor access to your PBX to conform to the needs of your business. Block access to international and long distance numbers if your company doesn't have a business relationship with entities outside your local area. If this isn't practical, consider using "time-of-day" routing features to restrict international calls to day-time hours only.
- Whenever possible, limit remote PBX access to local calls during normal business hours. Be sure to restrict access after hours and on weekends.
- Delete all authorization codes that were programmed into your PBX for testing and servicing.
- Assign codes on a need-to-know basis. Advise employees to treat codes as they would credit card numbers. Never print codes on billing records.
- Audit and frequently change all active codes. Cancel unassigned codes, especially those used by former employees.
- Consider implementing a barrier code system, an additional numeric password that adds a second level of security.