

Protect your PBX!

Theft of long distance service, telecommunications services and toll fraud come in many different forms. Understanding your telecommunications system and the techniques used by the criminals are key to limiting your vulnerability to this type of crime.

1. Learn about your telecommunications system:

- know the safeguards, the inherent defenses and security features;
- determine the vulnerabilities;
- ensure staff are trained in safeguards and procedures.

2. Know the access paths that open doors to fraud:

- Direct Inward System Access (DISA);
- Voice-Mail System;
- Remote System Administration (Maintenance Ports);
- Direct Inward Dialing;
- Tie Trunks and Tandem Network Services;
- Modems.

3. Monitor and analyze your systems information:

- Study call detail records and review billing records (exception reports may provide a warning sign);
- Know calling patterns and review them;
- Review voice-mail reports;
- Monitor valid and invalid calling attempts whenever possible.

4. Know the signs of a security breach:

- Complaints that the system is always busy;
- Sudden changes in normal calling patterns such as increases in wrong number calls or silent hang-ups, night, weekend and holiday traffic, 800 and WATS calls, international calling, and odd calls (i.e. crank/obscene calls);
- Toll calls originating in voice-mail;
- Long holding times;
- Unexplained 900 (Chat Line) calls;
- High tolls for any unauthorized trunk extension.

5. Secure your System(s):

System configuration:

- Restrict access to specific times (business hours) & limit calling ranges;
- Block all toll calls at night, on weekends and on holidays;
- Restrict call forwarding to local calls only;
- Block all 10XXXX calling from your PBX if this service is not necessary
- Block, limit access or Require attendant assistance to overseas calls;
- Establish policies on accepting collect calls and providing access to outside lines;
- Educate switchboard operators and employees about "social engineering" (i.e. con- artists trying to obtain calling access or transfers through a PBX);

- Secure equipment rooms (lock up all telephone equipment & wiring frames);

PBX (Private Branch Exchange) and DISA (Direct Inward System Access):

- Change default codes after installation of new equipment;
- Never publish DISA telephone numbers;
- Change your DISA access telephone number periodically;
- Issue a different DISA authorization code for all users and Warn DISA users not to write them down;
- Do not use sequential access numbers;
- Use longer DISA codes (minimum 7-9 digits) and change the codes regularly;
- Disconnect telephone extensions that are not in use;
- Restrict DISA access at night, weekends and on holidays (Prime time for fraud);
- Block or restrict overseas access;
- Program your system to answer with silence after five or six rings (Hackers look for systems that answer with a steady tone)
- Identify invalid access attempts to your DISA and route them to an operator;
- Implement DISA ports that drop the line when an invalid code is entered;
- Program your PBX to generate an alarm when an unusual number of invalid attempts are made, and to disable the port after a set number of invalid attempts.

Voice-Mail Systems

- Establish controlled procedures to set and reset passwords;
- Change passwords regularly;
- Use maximum length passwords for system manager box & maintenance ports;
- Prohibit the use of trivial, simple passwords (i.e. 222, 123, your last name, etc.);
- Limit the number of consecutive log-in attempts to five or less;
- Change all factory installed passwords;
- Block access to long distance trunking facilities, and collect call options on the auto attendant;
- Block or preferably Delete all inactive mailboxes;
- Limit your out-calling;
- In systems that allow callers to transfer to other extensions, block any digits that hackers could use to get outside
- lines, especially trunk access codes;
- Conduct routine reviews of the status of your system and system usage.

Remote Access Ports

- Block access to remote maintenance ports and system administration ports;
- Use maximum length access codes and change them regularly.

Modems

- Use maximum length passwords and change frequently;
- Eliminate three-way calling on all extensions used with modems;
- Disconnect modems that are not in use.