

LOCK THIEVES OUT OF YOUR SYSTEM

They're called 'phone phreaks', 'dump bin divers' and 'shoulder surfers' and they cost businesses millions of dollars each year. They use corporate PABXs for personal gain and your system may be their next target. So what can you do to protect your system from toll fraud?

Get an education in toll fraud tactics – think like a thief

One of the best ways to help protect your company PABX from toll fraud is to learn how hackers gain access to your system so that you can block their entry. These perpetrators usually choose one of several methods of cracking a PABX.

Voice Mail - Accessing long distance destinations through a voice mail system

Someone outside your company can call into your voice mailbox, crack the long-distance access codes and dial out to locations around the world. You won't know until a 300-page phone bill arrives with hundreds of international calls on it.

Criminals also can gain access to your voice mail by remotely accessing the administrator's terminal to take over mailboxes for their own illicit purposes. Once they have access, they can exchange lists of long-distance codes, coordinate drug shipments and sell stolen bankcard numbers. And these activities are just the beginning.

DISA – Stealing DISA numbers and access codes

If your company has Direct Inward System Access (DISA), a feature that allows users in remote locations to place calls through your corporate PABX, you could be a target of toll fraud. Shoulder surfers may steal security and authorisation codes from company employees who are using pay phones in airports or other public places. Dump bin divers may steal lists of access and authorisation codes from the dump bin at a company site. In addition, hackers frequently set up computers to repeatedly dial numbers and access codes until they hit a correct combination.

Impersonation – Posing as technicians or telephone company employees

How secure is your switch room? If just anyone can walk in without being noticed or questioned, you may be the next victim of a more direct form of toll fraud attack. Criminals can pose as telephone company technicians and gain access to your corporate PABX, even from remote locations. A receptionist or someone inside your company may become an unwitting partner in crime if they provide access codes over the phone. Also, don't underestimate the importance of deleting employees' authorisation codes when they leave your company. If they bear any ill will, they may use or sell the codes as a means of getting revenge.

Use Nortel Networks' toll fraud protection tools

Nortel Networks ensures that a high level of security is built into every Meridian 1 system. However, as a system user, it is your responsibility to maintain your system's security and implement as many of its safeguards as possible.

Meridian 1 system software

Your Meridian 1 system software is your first line of defence against toll fraud. Keeping your system up to date with the latest release of software reduces your risk of falling victim to fraud. Once your system is installed, you need to ensure that your company is using all of the protective features that are built into your PABX. For example, you can use the Call Detail Recording feature to output authorisation codes as well as calling and called parties, and time and duration of calls. Including authorisation codes allows you to review call records and detect toll fraud initiated from both inside or outside your company.

Protect remote access ports to your Meridian 1 system by using the Limited Access to Overlays security features. These require both user identification and an alphanumeric password. You can then enable the invalid login attempt threshold to restrict hackers' attempts to guess passwords. Lock the port out for up to three hours and activate the audit trail to track who has been in your system and to see what they have accessed. Activate a 'Security Banner' for PABX remote access ports to alert those attempting illegal access that they are trespassing. It may not stop their attempt, but it serves as a warning and eliminates the defence of ignorance.

Another way to limit toll fraud is to restrict Call Forward to internal numbers only and to limit the number of Call Forward digits.

Direct Inward System Access

Your organisation may permit employees to access long distance services using personal authorisation codes even when they are on the road. At the same time, you need to keep those codes out of the hands of hackers and thieves. The first level of security you can establish for Direct Inwards System Access (DISA) is a security code. Using the Meridian 1 Security Code feature, you can require callers to enter a one- to eight-digit code to gain access to long-distance calling. The longer the code you require, the harder it will be for hackers to crack.

Once callers gain system access with a DISA code, the Meridian 1 system allows you to impose additional calling security measures. For example, you should require callers to enter a personal authorisation code in addition to the security code to use outgoing lines. DISA is a feature that is now available by request, rather than as a standard capability. If you have a Meridian 1 system and want to disable the DISA capabilities, contact your distributor. You may also want to consider the use of Network Speed Call to limit where DISA users can call.

Meridian Mail

Your voice mail system is another avenue for the perpetrators of toll fraud. However, you can minimise the risk of toll fraud by using features that control access to Meridian Mail and your Meridian 1 system. Criminals can seize control of your voice mail administrator terminal and mailboxes. To minimise unauthorised access, change your administration terminal password often and have users do the same with mailbox passwords. Force users to change their password on the first log-on to their mailbox. Remove unused mailboxes to keep thieves from moving in and setting up call sell operations.

Three features that can assist you in establishing a Meridian Mail security program at the mailbox level are Thru-Dial Restriction, Password Change and Invalid Log-on Attempts. Monitor your voice mail reports for suspicious activity. With each new release of Meridian Mail software, as with Meridian 1 software, new security features are added. Keeping your Meridian Mail software up to date also puts a lock on your system and gives you peace of mind.

Checklist for protecting your Meridian 1 system

- **Deny unauthorised access.** Thieves can access long distance facilities through your voice mail system. You can block thru dialling by ensuring access codes for external calling, special prefix codes and flexible feature codes are blocked.
- **Secure DISA numbers.** You should not publish DISA numbers. Require outside callers making incoming calls to a DISA line to input a security code and an authorisation code with as many digits as your company's corporate culture will allow. Don't use employees' extension, home phone or ID numbers as authorisation codes because hackers may be able to easily break these codes.
- **Foil the dumpster diver.** Don't throw out call detail records and credit card receipts. Dispose of these materials, including switch printouts and old documentation, as you would any proprietary material.
- **Change codes frequently.** Change authorisation and voice mail passwords and security codes as often as is appropriate for the user community. Delete codes of former employees. Change the passwords for Meridian 1 and Meridian Mail Administration terminals regularly. Also, change system passwords when key personnel with password knowledge leave your organisation.
- **Maintain secure authorisation codes.** Treat authorisation codes like credit card numbers. Don't allow employees to share authorisation codes. Use as many digits in an authorisation codes as possible for your user community.
- **Monitor calls.** Most toll fraud is generated in a short time. Monitor call detail records for suspicious calling patterns. Automatically output traffic reports that identify possible unauthorised access.
- **Restrict international calls.** International locations are the major destination for toll fraud calls. Restrict international calls if authorised users do not normally place calls to these locations. If users do place calls to international locations, allow only the area codes and country codes they require. Provide international calling capabilities only to users who require them and make sure you restrict Meridian Mail agents from making international calls as well.
- **Restrict Call Forward.** Program your system so that extensions cannot forward calls to long distance numbers.
- **Secure access codes and passwords.** Don't allow employees to post access codes and passwords in plain view.
- **Know who is in your switch room.** Secure access to your switch room at all times.

The security features available with your Meridian 1 PABX are your first line of defence against toll fraud. Third-party protective packages are available which can be used to monitor calling patterns (ie. a TIMS system). But most importantly, audit your system and make sure you use the features you have to prevent unauthorised access to long distance services. Your attention to system security can help make the surprise phone bill a thing of the past.