



Lock

thieves out of your phone system

Lock Thieves Out of Your Phone System

Get Educated In Toll Fraud Tactics.

“Think Security” and Protect Your Money

They're called 'hackers', 'phone phreaks', 'dump bin divers' and 'shoulder surfers'. They sell information between themselves and they cost businesses millions of dollars each year. They use weaknesses in corporate PABX programming for personal gain at the (considerable) expense of the victims and your system may be their next target. So what can you do to protect your system from toll fraud?

Get educated in toll fraud tactics

“Think Security” and Protect Your Money

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 can use several methods of hacking a PABX to reprogram it.

Why do they do it?

People like free things. A free phone call doesn't exist. Whether it's a hacked payphone or a cheap call to the home country via a series of PABXs and trunks across the world someone pays. Free phone calls are theft from someone else.

How do they do it?

Logins and passwords on a maintenance modem and the PABX will restrict remote access to only authorised parties. However, leaving these off or set to well-known default values will leave the way open for hackers anywhere in the world to remotely access and reconfigure the PABX, modify security and dialing parameters, design a plan to dial in and out of your system and return when you aren't suspecting anything out of the ordinary. The toll fraud perpetrators are experienced in the technology of all PABX and voice mail systems on the market. Don't let them get remote access to your system.

Direct Inward System Access (DISA) is designed to connect external diallers as if they are “inside” the company's PABX. DISA is usually used for after-hours, international

calls that can be made from home rather than staying back in the office. Password mechanisms for DISA allow secure operation but leaving them off exposes the company to toll fraud by hackers who discover or know of the DISA dial in number(s). Hackers gaining access to your system's programming core can also set up a password liberated DISA number without you knowing it. If you don't need it, have DISA removed from your PABX. If DISA is installed, regularly check (daily) if DISA has been activated.

Voice mail allows saving and remote retrieval of messages. Mailboxes also have a password to provide secure access. If a mailbox password is guessable and the system is not tightly programmed, a hacker might be able to reprogram the background data-base and operator number to obtain international access to use when they want it, just by dialing '0'. Transferring out of the mailbox means that the number can be re-used – in fact over and over until all the company's lines are in use. Stop hackers at the first stage by having secure mailbox passwords, change them regularly and delete unused mailboxes. Commencing right from a new installation, never allow default mailbox and administrator passwords to be retained in your system.



Succession 1000 Family

What do OWNERS do?

Decide What You Need From Your system.

PABX systems can restrict calls by numbers, time of day, country codes, etc. The owner must decide what suits their business and what procedures need to be in place to keep the system secure. When key communications or administrator staff leave does the system get checked? Stay vigilant, suspicious and keep records.

Monitor your call costs and destinations.

Know what your calls are costing. The marketplace offers telephone accounting and control systems of varying complexity and cost. The cheaper ones keep records and might calculate call costs. The more expensive ones control the PABX security and provide alerts with inbuilt, programmable toll fraud detection systems. A typical weekend toll fraud 'hit' with 20-30 trunks being used can cost as much as an employee's yearly wage – and being valid calls to your local carrier, the bills will be legally payable. Toll fraud is big business and it's organised. Businesses can go bankrupt on toll fraud bills. Know of irregularities well before the monthly phone bill arrives with any bad surprises. Ask your installer what steps to take if you suspect toll fraud.

Lock down the outgoing destinations.

Nortel Networks PABX systems have multiple, powerful measures to totally restrict calls to inside the local system – that's totally secure. Most toll frauds are enabled via poor administration practices and badly programmed parameters, usually based on customer requests.

Call your installer and jointly review what numbers are allowed and barred in your system. Adopt the philosophy of initially barring all outside calls and only opening up to places that are requested or approved, and keep records. This approach allows all the new services being added by carriers to be automatically excluded until they are specifically allowed. For forwarding calls to mobiles, this can be barred unless allowed to specified numbers. Use a quality process where positive action is in place to review each request.

Control physical security

Determine how secure is your PABX or computer switch room is. If anyone can walk in without being noticed or questioned, you may be the next victim of a more direct form of toll fraud attack. Provide escorts where necessary. Keep sensitive details of passwords, network diagrams and so on, out of sight.

Change codes and authorisations

Delete employee authorisation codes when they leave your company. If they bear any ill will, they may use or sell the important codes as a means of getting revenge. Secure the passwords of your own company and your clients.

Document a plan of action

Develop a formal action plan as a "Toll Fraud Counter-measures" policy in your



Meridian Option 11



Meridian Option 61C

company. Have procedures worked out to know who to contact (the company, the installer, the carrier, the users) for emergencies and what short term actions need to be taken. Work out what facilities can be cut in emergencies until security is restored.

Periodic auditing

It is prudent to have PABX systems audited at regular intervals to check for security weak points and how well the programming suits the needs of the company. Investigate the features of newer releases with your supplier.

Use Nortel Networks toll fraud protection tools

Nortel Networks ensures that a high level of security is built into every Meridian and Succession 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. Consider barring all calls and opening up only what is officially requested and approved via a change control process and records. That way, new telco features don't slip under your guard, for example new operator connect services that if not barred, by default are allowed.

Meridian, Succession and Business Communication Manager (BCM) system software
Your Meridian, Succession and BCM 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 the appropriate 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 PABX system by using the available 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 legally eliminates the defence of "ignorance". Hackers are impatient and won't spend their own money. Make it hard for them.

Another way to limit toll fraud is to restrict Call Forward to internal numbers only and to limit the number of Call Forward digits. If Call Forward External is needed, call forwards can be to individually specified numbers, especially mobiles, so it's still a powerful but flexible form of restriction.

Direct Inward System Access (DISA)

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/Succession/BCM Security Code and path restriction features, 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 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. To help customers enforce security, DISA is a feature that is now available by request, rather than as a standard capability. If you have a Nortel Networks system and want to disable DISA capabilities, contact your distributor or maintenance provider. You may also want to consider the use of Network Speed Call to limit where DISA users can call.

Meridian Mail and Call Pilot

Your voice mail system is another avenue for the perpetrators of toll fraud. However, you

“We spend our money and effort protecting our data systems and computer access. I never thought I’d lose money out of our phone system.”

can minimise the risk of toll fraud by using features that control access to Meridian/ Succession/ BCM. Remember, with Nortel Networks PABXs we can restrict calls to a total lock-down and open them up to your very specific requirements.

Force users to change their password on the first log-on to their mailbox and/or add a prefix as well. Remove unused mailboxes to prevent fraudulent operations within your system. NEVER allow users to have passwords that are related to their extension number (forward, backwards, etc), or simple keypad lines and diagonals.

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

Interactive Voice Response and Auto-attendant systems in your system.

These sub-systems assist digit based selection of facilities within the PABX systems. If they use thru-dialling, the destinations must be restricted to the intended parameters. All combinations of numbers that can be dialled in, especially “unused” numbers in a publicised menu need to be checked for confirming the return to a known safe point in the designed system.

Virtual ACD agents

Non-physical numbers are sometimes used in control of ACD queues. These numbers need to be access controlled in the same manner as the normal, physical numbers.

Checklist for protecting your Meridian/Succession/BCM 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 (Meridian/ Succession) 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 dump bin diver.** Don’t throw out call detail records and system drawings. Dispose of these materials, including switch printouts and old documentation, as you would any proprietary material via shredders or security disposal bins. Information like this will be paid for by criminal elements, so there are a lot of spies around – inside and outside your company.
- **Change codes frequently.** Change the 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 PABX system and voicemail 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 authorisation codes as possible for your user community.
- **Monitor calls.** Most toll fraud is generated in a short time – days to weeks, and usually after hours when detection is least likely. Monitor call detail records for suspicious calling patterns. Automatically output traffic reports that identify possible unauthorised access. Encourage employees to report strange language on voice messages and callers, especially out of hours.



- **Restrict international calls.** International locations are the major destination for toll fraud calls. Restrict international and interstate 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. For other systems make appropriate restrictions on the dialling class of service tables. Start by barring ALL international number then enable only those you need to dial. Consider time of day shutdowns (individual over-ride codes can be issued as required)

- **Restrict Call Forward.** Program your system so that extensions cannot forward calls to long distance numbers. Divert to mobiles only when they are known and are registered in the system, and restrict all others.

- **Secure access codes and passwords.** Don't allow employees to post access codes and passwords in plain view. Look under the terminal keyboards, etc for "the usual hiding places" – crooks will.

- **Know who is in your switch room.** Secure access to your switch room at all times. Use escorts and monitors if required.

- 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.

To quote a CEO (Comms) of a major, multinational bank after toll fraud was exposed and detailed to him, "*We spend our money and effort protecting our data systems and computer access. I never thought I'd lose money out of our phone system.*" The phone system DISA fraud had been in operation for over three years (poor administration checking) and cost the bank over US\$1million. They now have a toll fraud/billing/accounting system in place and changed their international phone system security standards and procedures to address PABX security issues.

Your attention to system security can help make the surprise phone bill a thing of the past.

Lock thieves out of your phone system.



Australia
Level 5, 495 Victoria Avenue
Chatswood NSW 2067
Australia
Tel: 61 2 8870 5000

India
403-405, 4th Floor, North Block
Manipal Centre, Dickenson Road
Bangalore 560 042
Tel: 91 80 559 2087

Indonesia
Graha Paramita, Level 8
Jalan Denpasar Raya, Blok D 2 Kuningan
Jakarta 12940 Indonesia
Tel: 62 21 252 2280

Japan
Gate City Ohsaki, East Tower 9F
1-11-2 Ohsaki, Shinagawa-ku
Tokyo 141-8411
Tel: 81 3 5740 1300

Korea
16F, Haesung 2 Bldg
942-10 Daechi 3 Dong, Kangnam-ku
Seoul 135-283
Tel: 82 2 3707 4600

Malaysia
Level 2, Annexe Block, Menara Milenium
No 8, Jalan Damanlela, Bukit Damansara
50490 Kuala Lumpur, Wilayah Persekutuan
Tel: 60 3 2080 8000

New Zealand
Level 16
396 Queen Street
Auckland 1036
Tel: 64 9 309 9052

Pakistan
Ground Floor, Evacuee Trust Building
Agha Khan Road, F-5/1
Islamabad, Pakistan
Tel: 92 51 287 0005

Philippines
Wynsum Corporate Plaza
Level 29, 22 Emerald Avenue, Ortigas Centre
1605 Pasig City Philippines
Tel: 63 2 580 5500

Singapore
151 Lorong Chuan #02-01
New Tech Park
Singapore 556741
Tel: 65 6287 2877

Sri Lanka
Residential Accommodation Unit 60/3/8
Sahasapura Housing Scheme
Baseline Road, Borella, Colombo 8, Sri Lanka
Tel: 94 7 533 1133

Thailand
323 Betagro Tower, 4/F
Viphavadi-Rangsit Road
Laksi Bangkok 10210
Tel: 66 2 955 0588

Vietnam
The Press Club
59 Ly Thai To Street
Hanoi
Tel: 844 934 4309

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireline Networks, Wireless Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at:

www.nortelnetworks.com

Nortel Networks, the Nortel Networks logo and the globemark design, Succession, Norstar, Meridian, Passport, BayStack, Optivity, Alteon, and Contivity are trademarks of Nortel Networks. All other trademarks are the property of their owners.

Copyright © 2004 Nortel Networks. All rights reserved. Information in this document is subject to change without notice.

Nortel Networks assumes no responsibility for any errors that may appear in this document.

NORTEL
NETWORKS
BUSINESS WITHOUT BOUNDARIES