

3. TOLL RESTRICTIONS

- **What level of long distance calling is required within the organization?**
 - It's important to determine the calling pattern needs within the organization. Is international calling required by everyone, or only a select few?
- **Have all appropriate toll restrictions been activated?**
 - Block all unnecessary country codes, area codes and local prefixes (NNX such as 976 as 4th, 5th and 6th digits of a phone number), as well as 1-900, etc. where appropriate.
- **Is there an audit trail or record to determine calling patterns? Is a local CDR (Call Detail Recorder) device used to record long distance calls?**
 - CDR records give a current view of toll calling patterns and help determine whether restriction tables are used as required.
- **Does the business make use of toll free numbers such as 1-800/ 866/ 877/ 888? Is inbound calling allowed from anywhere?**
 - Block all unnecessary area codes and country codes where possible.

4. ACCESS CODES

- **Do the access codes used appear in sequential order?**
 - All access codes used should be randomly selected so as not to be easily guessed. A minimum of 6 characters should be used for access codes or passwords, whenever possible.
- **Are there dormant access codes within the system?**
 - Deactivate codes not being used by current employees.

5. FEATURES

- **Are call forwarding restrictions used when appropriate?**
 - Call forwarding should be restricted to 4 digits when possible, to prevent forwarding to an external number. This prevents one of the most common types of toll abuse through the call forwarding feature.

6. TELEPHONE ROOM

- **Is the telephone utility room appropriately locked to protect the hardware of the PBX and its peripheral devices?**
 - The equipment room should be locked and an audit trail logging who has accessed the room should be maintained. Card access devices that have the employee scan a card, in order to gain access, can accomplish this.

FOR MORE INFORMATION

- **If you have any questions about Toll Fraud and Phone System Security, your communications integrator or your phone system provider should be your primary contact.**
- **Other good sources on this topic include reference documents from the US National Institute of Standards and Technology (NIST). They can be found at:**
<http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf> and
<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- **Ultimately, if you still have unanswered questions, you may contact us at FightPhoneFraud@cogeco.com**
Visit Cogeco's Business Solutions website :
[Ontario »](#)
[Québec »](#)



BUSINESS PHONE SYSTEM SECURITY QUESTIONS & ANSWERS

Unfortunately, telephony fraud is a reality in North America; Protecting your business against unwanted intruders is the best course of action in this ongoing battle.

It is critical that the owners/operators of commercial telecommunications systems (Key System/Hybrid Key System/Private Branch Exchange (PBX)/Voicemail etc) such as yours take the necessary steps to protect their businesses from exposure to this threat.

This advisory is intended as a proactive measure by Cogeco Cable to encourage all our valued customers to address this important matter. For your reference, the following question-and-answer scenarios outline some key steps that Cogeco recommends be followed. If the material below seems unfamiliar, please use this document to facilitate a discussion with your equipment provider or system maintenance experts.

As Cogeco has no control over the choice or configuration of telephony terminal equipment you attach to the Cogeco network, Cogeco accepts no liability, accountability or responsibility for any fraudulent toll calls that may occur as a result of your internal telecommunication systems being hijacked and in turn your phone lines being utilized for toll fraud calling purposes.

1. REMOTE ACCESS

- **Who accesses your PBX remotely? E.g.: Vendors, technical support within the organization, administrators, contracted support, etc.**
 - A comprehensive log should be kept to ensure that all remote access users are identified.
- **Is there an audit trail to identify who has accessed the PBX? Does the report identify time, date, user ID (Identification)?**
 - Logs should be kept identifying who has remotely accessed the PBX. Identifying the user, time and date, and if possible, event logs (transactions that occurred). Although not necessary to review these logs on a daily basis, they should be reviewed periodically. This log becomes especially important when investigating unusual activity.

- **What method of authentication is used prior to gaining access to the PBX?**
 - Authentication devices such as smart cards or other token authentication devices provide an additional layer of security.
- **Are remote access telephone numbers published?**
 - Access numbers, login procedures and passwords should never be posted/published.
- **Does the PBX terminate the call after 3 unsuccessful log-on attempts?**
 - After a recommended 3 attempts to log on to the PBX, if unsuccessful, the call should be terminated. This deters repeated unauthorized attempts.
- **Is DISA (Direct Inward System Access) used to access the PBX? If so, how are the access codes managed?**
 - If DISA is necessary the access code or password must be kept confidential, changed often, be the maximum number of characters (10-15 is recommended), and deleted immediately if no longer required.

2. VOICE-MAIL SYSTEMS

- **Are passwords a minimum of 6 characters?**
 - Passwords or PINs should be a minimum of 6 characters. It is desirable to use the maximum number of characters. The system should be set to accept no less than 6 characters.
- **Are passwords easily guessed or posted?**
 - Passwords should not be easy to guess, never posted nor shared. Don't use common number combinations such as the extension or the 7-digit telephone number. Software packages that test for common passwords should be used where possible.
- **Are passwords randomly generated when activating a new subscriber?**
 - Passwords should never be set to the telephone extension when assigned to a new subscriber.

- **Is the voicemail system programmed to enforce a password change every 30 – 90 days?**
 - Appropriate software should be utilized, prompting employees to change their passwords at least every 90 days. If the software is not available, then policies should be established, advising all employees of the importance of frequently changing their passwords.
- **Have unassigned mailboxes been removed?**
 - All mailboxes that are empty or unassigned should be removed. Vacant mailboxes are used for fraudulent purposes. Only current employees should be assigned a mailbox.
- **If shared or group mailboxes are used, how are they managed?**
 - Group mailboxes should have an individual assigned to manage it, by removing messages or ensuring that the greeting has not been changed.
- **Is the capability of through-dialing used, and if so, how is it managed?**
 - If the capability of through-dialing is not necessary this feature should be disabled. Significant fraud occurs by using this feature within the voicemail system.
 - If the feature must be used, daily reports for through-dialing should be monitored, especially after hours and during weekends. In addition, typical outgoing trunk access codes should not be used, such as 9, 8, 9+0, 9+1, 9+011, 9+1-800/866/ 877/ 888 etc.
- **Are the voicemail system reports monitored to ensure unauthorized access has not occurred?**
 - Reports that demonstrate port activity should be reviewed often. This will determine if there have been unauthorized attempts into the voicemail system as well as toll abuse.