How to protect yourself from toll fraud

ThinkTel actively watches for any anomalous traffic on your phone lines, and will shut down any traffic to high cost or odd areas. But there are also steps you can take to protect yourself against toll fraud.

WHAT IS TOLL FRAUD?

Toll fraud is the theft or unauthorized use of long distance phone service. Toll fraud takes many forms but is especially prevalent to phone systems that have not been secure, or where lax security measures are in place. Toll fraud is a problem worldwide, and fraudsters can easily rack up tens of thousands of dollars in long distance charges before the phone's administrator is even aware of a problem.

HOW DOES IT OCCUR?

Fraudsters generally infiltrate your telephone system by using various techniques that help them guess the passwords for voicemail boxes. It is relatively simple for most fraudulent operators to access your telephone system if your passwords are easy to guess or if you haven't modified the default passwords issued when the telephone system was activated.

YOUR LEGAL RESPONSIBILITIES

Costs associated with calls placed on your phone lines are your responsibility, regardless of whether you authorized those calls or not. For this reason, it is imperative that you take steps to protect your company against toll fraud.

HOW CAN YOU PROTECT YOUR PHONE SYSTEM?

It is important to take steps against toll fraud. If you do not, it is only a matter of time before your company is victimized. This document will outline some general guidelines to protect your company against toll fraud, but we strongly encourage you to take any measures possible above and beyond what is listed here.

TOLL RESTRICTION: International locations are the major destination for toll fraud calls. It is recommended that your company blocks all international numbers and only enable calls to those places that you need to call. Some systems allow for passwords to be required for long distance calls. If this is a possibility, we recommend you change the passwords regularly, and especially when an employee has left the company.

GENERAL SECURITY: Follow best practices for all security, including monitoring resources for vulnerability, maintaining patches and reviewing logs. Consider utilizing standards-based security add-ons where possible.

AFTER-HOURS CALLS: Restrict all outbound after-hours calling.

LIMIT ACCESS: Limit system access to authorized personnel only, even during company business hours.

PASSWORDS: Immediately change the default passwords provided with your phone systems, and include password changes as part of your regular maintenance, and when personnel leave your company. Require complex passwords.

UNUSED MAILBOXES AND PHONES: Proactively disable mailboxes and remove all access to outgoing employees immediately. This is not only to protect against retaliation from disgruntled former employees, but also against anyone who may obtain that person's security information.

EXTERNAL TRANSFER: Restrict call forwarding and call transfer features, especially to external numbers. Program your phone system so that extensions can forward only to known numbers, and restrict all others. Never forward a caller to 901 or 90#.

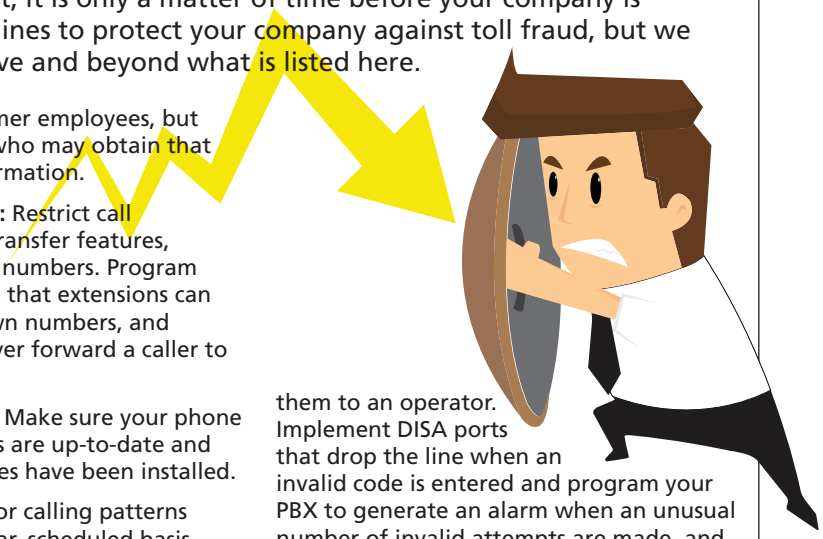
SOFTWARE PATCHES: Make sure your phone and voicemail systems are up-to-date and that all current patches have been installed.

MONITORING: Monitor calling patterns and usage on a regular, scheduled basis. High costs can be generated in a very short period of time and will continue until action is taken to stop it.

BLOCK COLLECT CALLS: Block the system from accepting revers charges on telephone calls - opt for a toll-free number instead.

DISA NUMBERS: Never publish any phone numbers that could provide direct access to your system (DISA). Change your DISA numbers periodically, and issue a different DISA authorization code for all users. Warn users to never write down their authorization codes.

INVALID ACCESS ATTEMPTS: 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 and 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.



MODEMS: Eliminate three-way calling on all extensions that use modems. Physically disconnect modems that are not in use.

FIREWALLS: Restricting access to your SIP port(s) on your PBX at a IP address or subnet level is an effective way of reducing your exposure to indiscriminate port scanning bot networks.