

Actimax PLC

Preventing Toll Fraud

The best defense against toll fraud remains an educated customer. Actimax, working with its carrier partners is totally committed to the control of toll fraud. While no telecommunications system can be made entirely free from the risk of toll fraud, diligent attention to system security can reduce that risk considerably.

- [Teach Your Employees Well](#)
- [Mind Your P's, Q's And Numbers When Choosing Passwords And Access Codes](#)
- [Change Passwords And Codes Often](#)
- [Take More Control Of Your Long Distance Calling](#)
- [Learn To Spot Suspicious Incoming Calling Patterns](#)
- [Check Your Voice Mail](#)
- [Slam The Door On Automated Attendant Crooks](#)
- [Monitor, Monitor, Monitor](#)
- [When All Else Fails, Swing Into Action](#)

Teach Your Employees Well

Keep your employees informed. Since one of the leading causes of toll fraud is theft of access authorization codes and passwords, make sure your people guard these numbers carefully. Instruct them never to write these numbers down or program them into auto dialers.

Warn traveling executives that thieves may be watching from afar with binoculars or lurking at adjacent pay telephones when they make a call, trying to obtain their access codes or calling card numbers.

In addition, instruct employees to verify the identity of someone placing a collect call to your company before accepting the charges (you may even want to institute a password for salespeople or other employees who may call collect).

And warn everyone in your company about one of the fastest growing toll fraud tactics - the seemingly innocent incoming caller who asks to be transferred within your system. This person may, in fact, be a thief using deceit to enter your network and gain access to an outside line. It's a good idea to direct your employees to immediately report both suspicious behavior on the part of callers asking to be transferred, or a sudden increase in the number of requests for transfer.

When all is said and done, the more your employees know about telefraud, the easier it will be to enlist them in the effort to prevent it.

Mind Your P's, Q's And Numbers When Choosing Passwords And Access Codes

One of the most effective ways to stymie crooks is to select hard-to-break passwords and remote access codes. Rule number one: use the maximum number of characters. To make a crook's life more difficult, it makes sense to avoid passwords which contain the following:

- Predictable patterns, like ascending or descending digits
- The same digits (5555555)
- The same number as your extension (or your extension reversed)
- Align numbers that identify the owner (room number, employee ID # or even a social security number).
- And please don't use default passwords or default access numbers - they're easy to crack as almost everyone knows them.

Change Passwords Often

It's a good idea to change passwords a minimum of four times a year. Change or remove authorization codes when authorized users leave the company, especially when technicians depart. Never, never, write down remote access codes or passwords, or program them into auto-dialers.

Take More Control Of Your Long Distance Calling

Since placing unauthorized long distance calls is the goal of most thieves, the more controls you place on long distance calling the more secure your system will be. Some suggestions include:

- Prohibit or restrict calls to countries you do not do business with
- Limit international calling to only those employees who need to place international calls. Limit calls to domestic area codes if calls to these areas are not permitted
- Put time of day restrictions into effect, such as prohibiting or limiting outbound calling at night

Learn To Spot Suspicious Incoming Calling Patterns

In addition to fraudulently obtaining access to your Private Branch Exchange (PBX), one of the fastest growing ways thieves are trying to obtain an outside line is by deceiving your operators or employees. They may enter your system through a local access number or your 0800 service, then ask to be passed back and forth, eventually obtaining an outside line. We recommend directing switchboard operators to report unusual incoming calling patterns, including the following:

Callers repeatedly dialing in and asking for an invalid extension

Excessive hang-ups

Obscene calls

Wrong numbers

Callers asking employees what number or party they've reached

Dead air calls (incoming calls where the caller remains silent and waits for a hang-up)

Although seemingly innocent, each of these is a technique used by thieves to gain access to an outside line.

Check Your Voice Mail

Experienced toll hackers can connect to a voice mail system and access private bulletin board messages, create their own mailboxes, or may repeatedly transfer within the Private Branch Exchange (PBX) until they succeed in finding an outside line. Defensive measures include limiting voice mail to internal calling only, removing mailboxes immediately when an employee leaves, and avoiding spare mailboxes before they are needed.

Since voice mailbox security is provided by personal identification numbers (PINs), require users to change their PINs regularly. Make sure they use the maximum number of randomly generated digits in a PIN to reduce the odds of a hacker cracking a code.

And never, ever publish a list of remote access telephone numbers.

Slam The Door On Automated Attendant Crooks

After remote access and voice mail, automated attendants are the most common entry point for "telecrooks". They automatically answer a company's telephone, but can also serve as an open door to toll fraud. Telethieves enter the automated attendant function, then dial the 90XX or 900 extension.

On many Private Branch Exchanges (PBX) and voice mail systems (with dial-out capabilities left active), these extension numbers connect to outside long distance lines. To reduce automated attendant fraud, restrict or block access to long distance trunks and local dial capabilities. In particular, block access codes such as 900XXX.

Monitor, Monitor, Monitor

Continuous monitoring of your company's calling patterns will help you to identify fraud at an early stage and minimize loss. It's a good idea to regularly monitor Private Branch Exchange (PBX), voice mail, automated attendant and call detail records.

Learn to spot patterns such as an increase in after-hours calls, calls to countries you don't do business with, multiple short duration inbound calls (especially after working hours) and incoming calls from suspect areas. Keep a sharp eye out for numerous incoming calls on your 0800 lines followed shortly thereafter by a surge in long duration outbound calls - a tip-off that thieves are entering through your 0800 lines and then dialing out.

When All Else Fails, Swing Into Action

If, despite your best anti-fraud efforts, you suspect - or actually detect - tampering, that's the time to take action. Unlike calling card fraud, there is no limit to the potential for loss and complete liability in the event of toll fraud. And since toll fraud charges can mount fast, you can't afford to lose a minute.

Your first two calls upon suspecting fraud should be to Actimax and your line/Least Cost Routing provider. Together, we can begin to pinpoint the fraud source and block further fraud attempts.

You can never eliminate the risk of fraud. But you can be prepared if and when it occurs, and thus minimize the damage to your company's operations and finances. One thing you can almost count on - when fraud happens it won't happen at a convenient time. These criminals often will direct their heaviest assaults on your network when vigilance is at its lowest, during non-business hours, in the middle of the night, on weekends or holidays. That's why it's a good idea to have ready a Crisis Intervention Plan (CIP). It should contain a checklist of actions you can take the moment you spot fraud. With a CIP in hand, you can minimize the time necessary to stop fraudulent calling, and perhaps even stop the telethieves in their tracks.

Actimax will change all System Default Passwords and ensure that any manufacture recommendations to prevent toll fraud are implemented on your telephone system.

Actimax strongly recommends that the customer include the telephone system and related applications as part of their company security policy.

Actimax will not be liable for any costs incurred due to toll fraud of any kind and has taken all possible actions to prevent such incidents.

Should you wish to discuss further please contact the Actimax Service Department.