












Generic Guidelines for Preventing Toll Fraud

Preventing Toll Fraud

We believe that the best defence is to educate our clients about the risk of toll fraud.

360 Solutions and our carrier partners are totally committed to the monitoring and prevention of toll fraud. However, due to the fact that no telecommunications system can be configured to be entirely immune to the threat of toll fraud, if close attention is paid to system security, we can help you substantially reduce the risk.

-  Educate your employees about Toll Fraud
-  Choose Effective Passwords And Access Codes
-  Change Passwords And Codes on a Regular Basis
-  Control Your Long Distance Calling and Premium Rate Destinations
-  Learn To Spot Suspicious Incoming Calling Patterns
-  Check Your Voice Mail
-  Slam The Door On Automated Attendant Crooks
-  Continuous Monitoring
-  If all else fails - Take Action!

Educate your employees about Toll Fraud

Keep your employees informed.

Theft of system access / authorization codes and passwords is one of the most common methods of carrying out a toll fraud attack. For this reason, employees should be aware of the importance of guarding these numbers carefully – with them almost being the equivalent of their debit / credit card PIN number. With this in mind, they should never to write these numbers down; program them into auto diallers or assigned to mobile phone speed dial keys.

Mobile employees must be vigilant when accessing the system remotely, as it has been known for thieves to obtain access codes and calling card numbers through watching as the digits are entered – this is much the same as how bank related fraud is carried out so the same protective measures and precautions need to be applied.

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).

It is also vital to warn ALL employees that all incoming callers must be screened before being transferred within your system – do not transfer a caller without knowing who they are – and if they purport to be from the system maintenance company – please ask them for some evidence / credentials. This is because thieves will often deceive the switchboard in order to gain access to an outside line.








Please encourage employees to report suspicious behaviour immediately. They need to be particularly vigilant about callers asking to be transferred without specifying a name, or if there is a sudden increase in the number of transfer requests.

So just to reiterate - the more educated your employees are about the threat of toll fraud (also known as phone phreaking and telefraud) then the easier it will be to enlist them in the effort to prevent it.

Choose Effective Passwords and Access Codes

One of the most effective ways to prevent toll fraud is to select hard-to-break passwords and remote access codes. Rule number one: use the maximum number of characters.

Please 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)
-  Don't use default passwords or default access numbers - they're easy to crack as almost everyone knows them.

Change Passwords on a Regular Basis

Please 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 write down remote access codes or passwords, or program them into auto-dialers.

Control Your Long Distance Calling and Premium Rate Destinations







Since placing unauthorized long distance / premium rate calls is the goal of most thieves, the more restrictions you place on expensive calls, then the more secure your system will be. Some suggestions include:

-  Prohibiting or restricting calls to countries you do not do business with
 - Limit premium rate calls to those employees that have a need to make such calls as part of their job role.
-  Ensure that any class of service permissions match employee seniority
-  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 dialling 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 can be 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 using 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 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 hackers. They automatically answer a company's telephone, but can also serve as an open door to toll fraud. Once hackers have entered the automated attendant function, they will then try and 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.



Continuous Monitoring

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 dialling out.

If all else fails – take 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 system maintainer and your line/Least Cost Routing provider. Together, they 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 minimise 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 will often 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 thieves in their tracks.

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

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

360 Solutions 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 this further please contact the 360 Solutions Support Team on
0845 2239360**