**Suggestions for Guarding Against Toll Fraud**

Phone systems have many features included. Some users may use all features included in the phone system. Some phone systems are left with open features that will not be used such as ports, call transfer, call forward, call notification, short mailbox passwords, no time limits on either incoming or outbound calls. 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. Since this equipment is not owned, sold, managed or maintained by Time Warner Cable, it is the responsibility of the business to implement security measures against potential threats.

Most recent reports of telecommunications fraud have occurred around onsite Private Branch Exchange (PBX) systems, by using direct inward system access (DISA). Fraudsters gain entry to businesses utilizing PBX-based voice and phone systems and leverage system commands (like 800, 1010 Casual dialing numbers) or other forms of access numbers to establish a dial tone seeking to resell long distance for profit which can lead to high long distance charges.

Some companies’ internal IT personnel and/or phone vendor companies have shared some of their steps taken to secured and/or prevent phone hacking. Below you will find some of the steps that have worked in the past for companies when securing their PBX.

Voicemail Systems –

Systems that provide out-dial or through-dial capabilities are a popular way to gain access to your phone system to make fraudulent calls. By transferring out of a system, intruders can place long distance calls. Trespassers also look for default codes on mailboxes so they can change the codes and control the boxes.

Private Branch Exchange (PBX) -

A Direct Inward System Access (DISA) permits convenient access to a PBX from a phone outside the business via an 8XX number or other special access number so that authorized persons can bill long-distance calls to the company's PBX. The DISA gives criminals the same opportunity, as well as the chance to set up a call-sell operation (in which criminals sell domestic and international telephone calls) at the company's expense.

Social Engineering –

Hackers have been known to use a company’s employees to obtain just enough information to seek out vulnerabilities. A company can inform their receptionists and secretaries not to transfer any callers to the outside line extension or prefix as this is almost an immediate giveaway of an attempted attack.

Refrain from providing extensions to unknown callers. This prevents a hacker from building their own company directory and targeting senior management or specific voice mailboxes since they can likely view a website or other published data to assist them when looking for vulnerabilities.

Raise office awareness of historic and current calling scams to prevent release of company sensitive information or internal phone numbers and extensions.

*For example* - Telephone companies or law enforcement officials will rarely ask customers to be a part of a testing procedure. Telephone technicians can conduct tests without the customer's assistance. If you receive such a request, tell the caller you will call them back so they can test.

Be suspicious of unknown callers asking your cooperation in “testing the telephone line.” Probe the caller for information such as employee ID number, supervisor's name, or call back number.

Suspicious Activity -

* In general, you should review your call detail records regularly and always be alert to signs of PBX abuse.
* Although seemingly innocent, some of these techniques have been used by hackers to gain access to an outside line:
* Repeated calls of short duration
* Unexplained increases in incoming or outgoing calls
* Sudden increases in 8XX usage, 1010XXX, etc.
* Changes in after-hours calling patterns
* Callers repeatedly dialing in and asking for an invalid extension
* Excessive hang-ups
* Wrong numbers
* Callers asking employees what number or party they've reached
* Incoming calls where music is playing

Tips to combat PBX Fraud

* Don't allow unlimited attempts to enter your system. Program your PBX to disallow access after the third invalid attempt, voice mail access or barrier code attempt. Disable external outbound international, long distance and local call transferring.
* Directories and business cards that list PBX access numbers should be shredded before being placed in the trash.
* Never give out technical information about your system to callers unless you are certain of the identity of the caller.
* Educate employees about the dangers of phone fraud and what they can do to help prevent it.
* Contact your PBX administrator, PBX maintenance provider and notify your phone provider to report any suspicious incoming or outgoing calls.
* Dead air calls (incoming calls where the caller remains silent and waits for a hang-up)

PBX Management

* Limit the number of employees who use remote access.
* Use an unpublished number for remote access lines instead of 8XX numbers.
* Your PBX could be programmed to wait at least five rings before answering a call.
* A steady tone used as a remote access prompt leaves your system vulnerable to perpetrators' automatic dialing programs. Use a voice recording or silent prompt instead of a tone.
* You could tailor access to your PBX to conform to the needs of your business and disable features that your business does not use or need.
* Block access to international and long-distance numbers your company does not call. If this isn't practical, consider using "time-of-day" routing features to restrict international calls to daytime hours only.
* If your company does not make international calls, use 1010 casual dialing or use the operator to make calls, consider blocking these abilities within the PBX.
* Your PBX could be programmed to provide additional authentication using access codes for employees or phone lines that you have designated to be used for making international calls.
* Restrict the Automated Attendant
* Despite the intentions of technology to increase productivity and make life easier for employees and consumers alike, auto attendants that permit callers to automatically be transferred to any given extension or department (without the use of receptionists) often serves as an open gateway for telecom fraudsters. Professional telecommunication thieves will enter the system via the automated attendant and then dial the 91XX or 9011 extension.
* On most PBX and voicemail systems, three extensions are capable of accessing the outside long-distance line. This can be mitigated by restricting or blocking access to long distance trunks and local calling features. Specifically, disable access codes such as 9XXX and possibly even 8XXX.

Preventing VOIP (Voice Over IP Protocol) Fraud

* Eliminate or reduce inbound or outbound call redirects, transfers and forwards to long distance and international numbers without proper authentication.
* Use a firewall with a VoIP phone system to only allow VoIP/IP access to pre-authorized IP addresses.
* Secure or disable all maintenance ports as this provides “back door’ access to your telephony network and could also potentially allow access to your private and confidential data as well since most VoIP phone systems use the same data connection or Internet Service provider.
* Hackers may also target modems attached to the service PORT of a PBX. This is provided by PBX manufacturers to allow remote support of the PBX. Typically, the connection should be opened

only when an authorized request goes from the PBX customer to the PBX vendor, but many PBX customers keep the connection always open and become vulnerable to attack.

* Use the latest encryption available for the phone system and firewall. Only allow access to IP addresses that have been designated by your IP PBX administrator.
* Frequently monitor your manufacturer’s website for any software or firmware upgrades as hackers usually find vulnerabilities posted in these forums or support sections when updates are needed.

Access Management

* Whenever possible, limit remote PBX access to local calling during normal business hours. Be sure to restrict access after-hours and on weekends.
* If applicable, disable I-RAD (Internal Remote Access Device) to prevent access to view and change programming with remote administration software or incoming calls that would allow the phone system to be programmed by an outside device or computer connected to a modem.
* Always change all default passwords. Assign codes on a need-to-know basis. Advise employees to treat codes and passwords as they would credit card numbers. Never print codes or passwords on billing records.
* Assign the longest possible authorization numbers your PBX can handle. Select codes at random, don't use telephone extension numbers, employee ID numbers, social security numbers, addresses or other common numerical sequences. If practical, limit or eliminate remote access to your PBX. If you eliminate remote access, make sure the system is disabled when not in use.

Tips for Preventing Voicemail Fraud

* Learn all you can about the features of your voicemail system. Audit and frequently change all active codes in your PBX that may have been used for testing or servicing. Immediately deactivate access codes and voicemail passwords of departing employees.
* Remove all mailboxes from your system that are not in use.
* On voicemail systems that provide out-dial or through-dial capabilities, always be sure to change any default authorization codes to prevent unauthorized access to local, long distance and international services. If you have to document passwords, authorization codes and access codes, limit this information to your PBX vendor, business controller and/or PBX administrator.
* Assign PIN numbers randomly and change them periodically, using the maximum number of digits your system will accept.
* Ask your vendor to perform random or scheduled system testing, diagnosis and maintenance on site instead of remotely.
* Your voicemail system could have a different three-digit prefix than your PBX.
* Never publish the remote access phone number that connects callers to your voicemail system.
* Your system could be programmed to terminate access after the third invalid attempt.
* Examine call detail records on a regular basis to highlight potential voicemail fraud.
* Develop a plan to both prevent and react to voicemail fraud. Share this plan with your employees and make sure they know what to do and who to contact if your system is compromised.
* When selecting voicemail passwords, ensure that access passwords are 6-8 digit combinations and are not easily guessed. Example: 1111, 1234, 123456
* Each password should automatically expire in 60 days or less.
* Access to the voicemail and administrative system could be revoked after three (3) failed login attempts and notification sent to your PBX vendor or phone system administrator.
* Through-dialing could be disabled unless absolutely necessary. If through-dialing must be active, detailed reports should be generated and monitored daily.
* All overseas long-distance calling could require end-user authorization and a code that is distinct from all other voicemail access codes.