ARE YOU AT RISK?

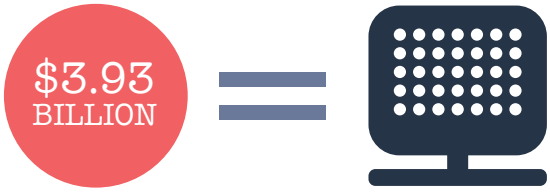
Protect your business from Toll Fraud

Telesystem
www.telesystem.us

Avoiding Long Distance Fraud

Across the globe, theft of long-distance voice services is occurring to businesses of all sizes. Whether a home office or large enterprise, chances are your business uses line services attached to phones or a PBX (Private Branch Exchange). **This means that you are vulnerable to Toll-Fraud that involves an unauthorized third party gaining access to your phone service and placing costly long-distance calls.** This can happen quickly! Within hours, your business could incur thousands of dollars of fraudulent calls. According to the Communications Fraud Control Association, fraud losses accounted for $38.1B in 2015.

Total cost in US dollars of global telecommunications fraud in 2015.



Total cost in US dollars of PBX hacking over the same period.

How do they do it!?

Fraud criminals most often call a business after hours, and then implement a variety of techniques to guess at passwords used to protect access to voicemail equipment, such as Private Branch Exchange (PBX) systems. If these passwords have not been changed from their default settings, or if passwords used are easy to guess (such as 1234 or 1111), it is fairly easy for these criminals to gain access to voicemail equipment, or other telecom fraud. Once inside, long-distance calls are initiated, resulting in unexpected charges.

As a subscriber, you are responsible for all calls originating from or charged to your telephone line. This applies to all customers, no matter who made the calls or accepted the charges. However, you can protect yourself. Start by adopting good telecommunications habits, and if you notice any suspicious activity on your line, contact the authorities, your vendor (if applicable) and your long distance provider at once.

Types of Fraud

Voicemail Fraud

Voicemail Fraud can occur by the hacker calling into your voicemail system and searching for mailboxes with weak or default passwords. Once in your system the hacker can change your voicemail settings that will allow them to place a collect call to the international number. They can also use your call forwarding program to forward calls to an international number, then use it to make calls.

We urge you to take the following additional steps to ensure your voicemail system is secure:

- Ensure all voicemail access passwords are 9-16 digit combinations and employees do not use easily guessed combinations. This includes temporary voicemail boxes.
- Ensure the voicemail access passwords expire after 60 days.
- Ensure the voicemail and administrative system access is revoked after 3 failed login attempts requiring a hard reset.
- Ensure all unused voicemail boxes are deleted from the system.
- Ensure through-dialing is disabled unless it is absolutely required. Through-dialing is the feature which allows for local and long-distance calling from within a mailbox.
- Ensure that if through-dialing is enabled, that its usage generates a report that is monitored daily to ensure no abuse has occurred.
- Ensure that overseas long-distance calling requires a unique end user authorization (Class of Service – COS) code which is different from the voicemail access password and restricts access after 3 failed attempts.
- Disable voicemail features not in use, such as call-forwarding or auto-attendant.

PBX Fraud

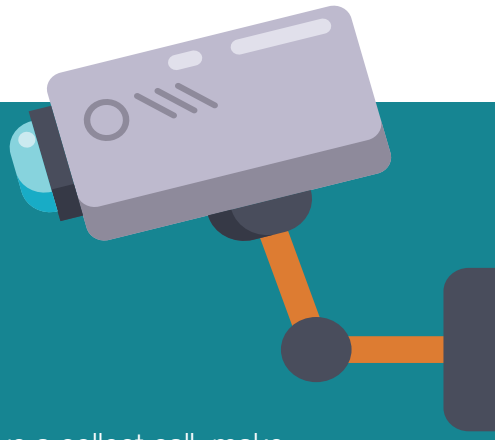
The majority of recent fraud cases have occurred around premise based Private Branch Exchange (PBX) systems, by direct inward system access (DISA). Intruders gain access to businesses that use a PBX phone/voicemail system and use system commands such as an 800 number or other access number to gain a dial tone. They place unlimited long-distance calls directly through these lines for unscrupulous operators reselling long-distance at a profit. These calls appear no different to the service or equipment providers than any other call originating from that business.

We urge you to take the following additional steps to ensure your voice communications are secure:

- Ensure your phone system is up to date with all releases and/or patches.
- Create strong passwords for your auto-attendants, suggesting 9-16 digits.
- Remove 3-way calling features on your phone system.
- Disable the remote/DISA programming access (port used by your phone vendor to gain remote access for programming purposes – this would be managed by your phone system vendor).

Modem Fraud

Be careful when surfing the web. Some sites will try to draw you in with a free offer, and then secretly download a program known as an Internet auto-dialer. The auto-dialer commands your browser to dial a long distance number - and you get billed for the call.



Monitoring Activity

Control Long-Distance Calling

Check your monthly phone bill carefully for any unusual charges. If you receive a collect call, make sure you know who the caller is, otherwise don't accept it. Don't let strangers use your phone.

Restrict Automated Attendant

Automated attendants that allow callers to be automatically transferred to an extension without the intervention of a receptionist can also serve as an open door to telecom fraud. Telecom thieves/ hackers enter the automated attendant function, and then dial the 91XX or 9011 extension. On many PBX and voicemail 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 9XXX and possibly even the 8XXX fields or install a "verify extension field" capability, if available.

Monitor and Analyze Your System

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 your PBX, voicemail, automated attendant and 800 call detail records. Learn to spot patterns such as an increase in after-hours calls, calls to countries you don't do business with and multiple short duration inbound calls (especially after working hours). Watch for numerous incoming calls on your 800 lines followed shortly thereafter by a surge in long duration outbound 800 calls, which may indicate that an unauthorized third party has entered your phone system through your 800 lines and is dialing out.

While this cannot guarantee your phone system will not be compromised, these additional steps can help deter hackers from targeting your system.

How to Protect Yourself

Businesses that take precautions against toll fraud will likely prevent perpetrators, thereby avoiding the cost and hassle of dealing with unauthorized phone system access.

Here is a simple checklist to help protect your company from unwanted access and fraudulant charges:

1 Passwords

- Never use the default passwords for voicemail, system administration, conference bridges, etc.
- Use passwords that aren't obvious or easy to guess, such as 1234.
- Enforce a policy of changing passwords on a regular basis.
- When someone leaves the company, delete their mailboxes immediately.
- Block or delete all inactive mailboxes.

2 Restrict Account Access

Determine what is necessary to conduct business and decide what level of restriction to apply to phones during normal and off business hours. You will be preventing fraud by controlling access to the account. Only authorized employees should be able to contact your phone system vendor and make changes to your account. Additionally, make sure your vendor maintains and adheres to the list of contacts and that one person in your company is authorized to change that list. You should also audit the list regularly to ensure that only the people you indicate can make changes to your account.

3 Health Check

Do a health check of your system regularly to monitor and analyze your systems. Work with your vendor and go through an annual audit to see if anything has been changed that might make you susceptible to toll fraud.

Regularly check your voice mail and auto attendant, as this can be the most vulnerable area for hackers to compromise and gain ability to make external calls. Consider disabling the ability to make external calls from the automated attendant system. A misconfiguration can be an easy target for hackers, so it's important to check the system and its security parameters frequently to make sure it's working correctly. Also, determine whether your voice mail system is authorized to dial out of the PBX itself or dial international numbers, as this is where most problems occur.

4 Monitor calling patterns

Monitor and review your call detail records. Check your voicemail reports, 800 number usage, monitor valid and invalid calling attempts and look for unauthorized 900 number calls. Also be on the lookout for changes in call patterns, such as a sudden increase in wrong number calls, silent hang ups, higher abandon rates, and an unusual amount of night/weekend/holiday.

5 Stay up to Date

Verify your business is utilizing all of the latest security releases. Make sure your phone and voicemail systems are up-to-date and that all current patches have been installed.

6 Upgrade to a Newer Phone System

Newer phone systems have increased security precautions built in. Older systems are much more vulnerable to being hacked, while newer systems and services were developed with security in mind.

7 Training and Education

It's important to educate and train your end users about what toll fraud is and how to prevent it.

How does Telesystem help your business avoid Toll Fraud?

At Telesystem we work to try to identify fraudulent activity and limit the liability to our customers. In addition to this information and customer education, we have monitoring tools that can assist at identifying various calling patterns that are different than those typically used.

These tools help, but they are by no means an end-all solution to preventing toll fraud, and no guarantee to completely preventing theft. Additionally, we partner with some long distance carriers that also implement tools to help detect these unusual calling patterns.

We must all do our part to ensure the network components or equipment used in the solution, that we are responsible for, are secure! By providing useful information and customer education such as this to our customers, and explaining how this activity happens, we are taking a proactive step towards reducing theft and toll fraud.

Another way to limit the exposure of fraudulent activity is to talk to your insurance agent about any fraud insurance policies that may be available to you to help offset any costs should you or your company fall victim to fraud activity.

For more information please visit the FCC website at:
https://www.fcc.gov/consumers/guides/voicemail-system-hacking

If you have any questions please feel free to contact our customer service department at 419-724-9898.

2700 Oregon Road | Northwood, Ohio 43619 | 419.724.9898

www.telesystem.us