Toll Fraud

Notice to our customers regarding Toll Fraud

- Beware of Toll Fraud.
- Toll Fraud is a crime against you. DSL Telecom isn't responsible for your Toll Fraud.
- You need to take steps to protect yourself from Toll Fraud.

DSL TELECOM DOES NOT WARRANT THAT ITS PRODUCTS ARE IMMUNE FROM OR WILL PREVENT TOLL FRAUD. DSL TELECOM WILL NOT BE RESPONSIBLE FOR ANY CHARGES, LOSSES, OR DAMAGES THAT RESULT FROM TOLL FRAUD.

What is Toll Fraud?

Toll Fraud is the unauthorised use of your phone lines, equipment, or services to make long distance calls that are charged to you. Toll fraud is an illegal activity similar to computer hacking. It is a global, industry-wide problem totalling over a billion dollars annually. Toll fraud takes many forms including fraud involving mobile phones, calling cards, pay phones, and long-distance fraud on calls placed through phone systems (PBX hacking). It is a large enough problem that many of the major providers of long distance telephone service have a separate department specifically for identifying and handling toll fraud issues.

The Global Problem

PBX Hacking or otherwise commonly known as Toll Fraud, continues to be the global scourge of the telecommunications sector, recent reports from the CFCA estimate the fraud value to be in excess of $4.96bn per annum.

Commonly regarded as white collar crime, decades of investigations remain open ended, leaving the environment ripe for repeat offenders.

The first symptom of PBX hacking generally occurs when the carrier notifies their client that their network is reporting surges in call volumes to international telephone numbers. At this stage, the carrier advises the enterprise to contact their PBX maintainer and have them lock down or shut off the PBX.

Accountability

The financial consequences of PBX Hacking generally kick off a frantic blame game, ultimately:

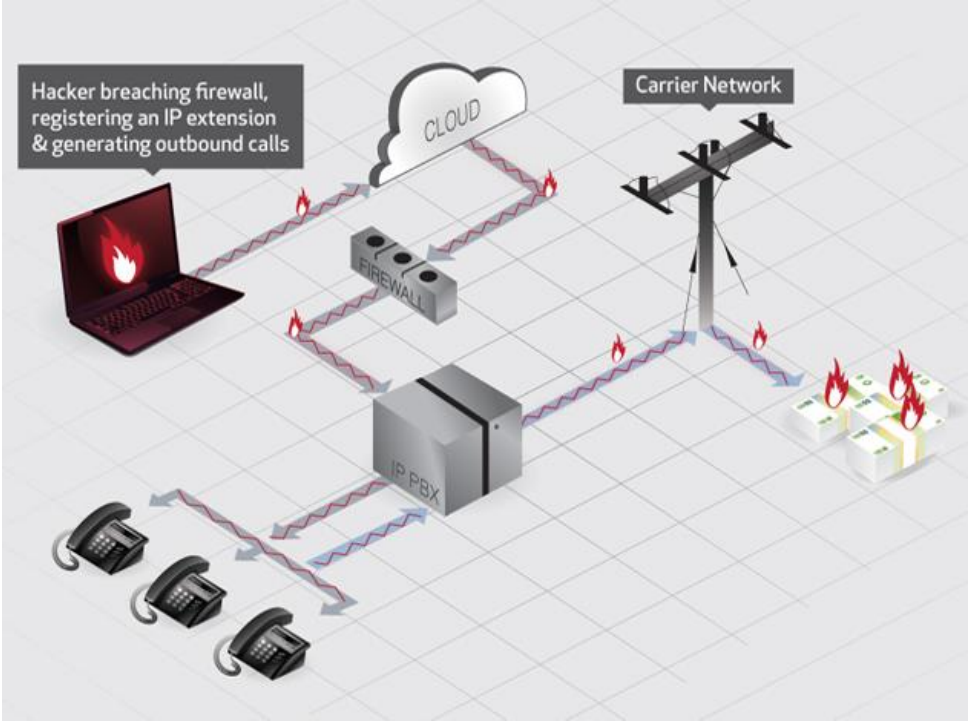
- The enterprise will demand that someone should be held accountable.
- The Carrier in question is legally entitled to collect their fees and the enterprise is legally responsible to pay the bill.
- Legal advice sought by the enterprise generally encourages them not to challenge a case that they cannot win.
- The VAR (PBX Vendor) argues that they cannot be held accountable for security breaches because they configured the PBX to their client's specification while also providing self-administration tools and training. The responsibility of network security always lies with the enterprise.
- The Police struggle to investigate due to lack of cross border regulation and international language barriers, resulting in zero prosecutions

The vast majority of reported cases result in:

- Very few prosecutions
- Accountability is never established
- Enterprise has to agree a settlement with the carrier
- The overall experience leaves the enterprise highly frustrated, financially exposed and vulnerable to further attacks.
- Trustworthy relationship established between Carrier, VAR (PBX Vendor) and client are often strained beyond breaking point.

Threat

The open world of unified communications (UC) and mobility applications increases the threat of hackers accessing your PBX system. Active PBX system features such as unified mobility, unified messaging, SIP account registration, call divert and conference facilities enhance the overall possibilities for a criminal to hack a PBX system. The correct security must be implemented and updated as new security updates are released.



FAQ's

Q. What is PBX Hacking? PBX hacking is a term used to describe a method used by criminals to illegally breach the security parameters of a PBX system.

Q: Why do criminals hack PBX systems? Criminals hack PBX systems for the purposes of accessing the trunk lines after which they begin generating as many calls as possible to expensive overseas telephone numbers off which the criminal collects 90% of this revenue.

Q. How does a criminal hack a PBX systems?

- Accessing the call divert functions within the voice mail and changing the routing number
- Log on to the remote maintenance port and re-configure the class of service tables
- Network access with brute force password attack
- Registering as a SIP account
- Working with internal staff members to manually divert an extension
- The list goes on

Q. Why do criminals make calls to expensive overseas number? Criminals register international premium rate numbers, all calls made to these numbers generate a significant profit for the criminal.

Q. How much is a call to an international premium rate number? Individual call costs average R50 – R200 per minute!!

Q. Who pays for the calls made to premium rate numbers? The owner of the trunk lines is billed for all calls.

Q. Why should an innocent party have to pay for calls they never made? The Carrier in question is legally entitled to collect their fees and the enterprise is legally responsible to pay the bill.

Q. Who are the perpetrators and why shouldn't they be prosecuted? The perpetrators generally reside outside the country. Due to lack of global regulation, language barriers and general cooperation, investigations remain open ended.

Understand your liability:

Under most long distance carrier agreements, if a call has originated with, or passed through a customers' equipment, that customer is responsible for the charges associated with the call, whether the call is authorized or not. This means that if you are the victim of toll fraud, you are liable for the costs. Learn how to prevent toll fraud because you have the final responsibility for securing both your phone system and any networked equipment in your business.

How to prevent Toll Fraud:

DSL Telecom wants to arm you with as much information as possible to help you avoid toll fraud. These guidelines will not completely eliminate the risk, but they can help reduce your chances of becoming a victim of toll fraud.

1. Restrict certain numbers or destinations e.g. premium rate, international calls on your phone system
2. Block international calls on your network's side (Telkom, Vox, Neotel etc.). If you need to make international calls we suggest using a Vox voice account for international calls as Vox is a lot quicker at detecting exposure and protecting their customer than Telkom is.
3. De-activate all unnecessary functionality
4. Analyse PBX call detail records for anomalies, out of office hours calls etc.
5. Restrict access to equipment e.g. : server room
6. Review procedures for leavers and vetting new recruits
7. Review and Update system security to identify potential weaknesses
8. Get DSL Telecom to upgrade your software if there are new security updates available. SLA customers will be notified and we encourage the customer to allow the technicians to upgrade the security settings.
9. Notify DSL Telecom should any changes be made to your network (for example changing your router/firewall, or adding new network devices so that any new potential vulnerabilities can be identified
10. Make sure your insurer covers you for cybercrime, specifically toll fraud insurance if the product exists.

But what do you do if your business is attacked?

- If you have been exposed the key is to limit any damage
- If you suspect your business is under an attack (engaged lines, constant dropped calls or your network provider notifies you) immediately turn off the power of your PBX and disconnect your lines at the wall. Contact DSL Telecom immediately.
- Contact DSL Telecom to log in and assess the breach, the passwords should be changed and assessment of any potential weaknesses can be addressed
- You will be liable for all calls made with your network. The best thing to do is not 'fight' with Telkom. Rather try negotiate a deal and they may be willing to minimise the amount that was fraudulently billed. A payment plan can usually be negotiated with your network provider.
- Try claim from your insurer if you are covered for this type of business risk. Many insurers do not understand this type of crime but generally it is an attack on your property which has resulted in loss.

DSL Telecom provides Service Level Agreements for our customers. As new releases of firmware with added security software is released we upgrade our customers that are on SLA to the new firmware version. While nobody can guarantee that you will never be hacked it is advisable to make sure you put up the best lines of defences to minimise your risk of becoming a victim. Updating security firmware regularly is one of these defences.

Common questions?

My phone company Telkom, Vox, Neotel etc. expects full payment for calls not made by our company, what argument can I provide to the phone company to get some relief on the bill?

As the phone company is the **"service provider"** for their clients, they should have safeguards in their Central Office to ensure that if they see an unusual increase in "minutes of use" (MOU) for their customers, they should shut down the phone lines, or at least inform their client. If your service provider is Vox, Vox does pick up irregular traffic quickly and will suspend the lines to limit the customer's exposure until a customer has either cleared the calling as regular or the customer has re-secured their network. Other networks can be slow to react. PBX toll

fraud is not a new problem and not doing anything about it in the network to protect customers from toll fraud is a lack of responsibility on the side of the service provider.

Should I get insurance, if it exists, to protect my company against PBX toll fraud and hacking?

We're not sure an insurance policy exists to protect against toll fraud. However, the mere fact that the Sony PlayStation network got hacked not once but twice in the last year shows how sophisticated hackers are getting. Think about that – Sony gets hacked and over a million customers have supplied their credit cards through Sony play station's to get their games, and Netflix movies, and the Sony engineers could not keep it from happening a second time? We believe Sony employs some pretty smart network engineers, but even they could not prevent hacking. So the answer is yes if such insurance exists, we recommend buying it. DSL Telecom is busy developing an insurance product for the South African Market and will be available soon.

What is DSL Telecom's position on PBX toll fraud and/or hacking, with regard to taking responsibility?

We do our absolute best to prevent hacking by including firewalls and software to detect bad logins (Built in the Firewall's), and follow best practice in the use of strong passwords. We will provide our best efforts in technical support to help prevent fraudulent intrusion into the PBX but ultimately the customer is liable (and not DSL Telecom or any of its agents for their own network if they are defrauded.

How can DSL Telecom and its resellers ensure that everything reasonably expected to protect the equipment against hacking has been put in place?

DSL Telecom staff members have been well trained in all aspects of security and work closely with its suppliers to ensure international best practice is implemented at each and every installation. We are aware of security threats and along with our technical partners inform our Resellers about this and how to take action to prevent hacking. We have also introduced Service Level Agreements for our customers which ensures that as a new security release or best practice comes out it is implemented at the customers site.

Watch this video on cybercrime in particular Toll Fraud: Click Here