innoTel.

TOLL FRAUD MINIMISATION INFORMATION

Toll Fraud, the practise of hackers gaining unauthorised access to a Private Branch exchange (PBX/PABX) or Phone System, in an attempt to obtaining free calls, stealing company information or cause damage to a business.

When attempting to obtain free calls, hackers often target international destinations and premium rate numbers, both with high costs associated with them and leaving you, the customer and bill payer a substantial phone bill.

This damage could result in very large phone bills, confidential information being accessed; additional costs related to security and have potential legal ramifications. In the United States alone, the cost of Toll Fraud is above $4 Billion annually and trends globally show that it is increasing each year.

Whose responsibility is protecting against Toll Fraud?

Yours. As and the owner of a service and associated phone system hardware, you are responsible for the upkeep and maintenance of your PBX or phone system, including its configuration, security and access.

Note: If hacking and fraudulent use of your phone system results in unauthorised call charges billed to your account, you are responsible for the equipment, service and as the account holder you are liable for any charges billed to you.

Toll Fraud is a concern for any business with a Phone System.

I've heard Toll Fraud is limited to VoIP systems?

No. This is not true. It is true that VoIP and the increasing number of VoIP PBXs have made it easier for hackers to gain access to phone systems due to poor implementation practises however, Toll Fraud can occur on any type of phone system and is not limited to VoIP. The reality is that all phone systems, when incorrectly implemented or configured, and poor user judgement, are at risk.

What are some of the signs of Toll Fraud?

If you are diligent in your checking and monitoring, the following are signs that Toll Fraud might be occurring.

- Outgoing call records may start appearing in customer toolbox. These will typically be;
  - Lots of short calls to international or premium rate numbers;
  - Calls to destinations you don't recognise;
  - Calls to the same numbers over and over; and
  - Calls made outside of business hours, or on weekends and public holidays.
- Access to make outgoing calls, or accessing/retrieving voicemail may fail or be delayed

If you have received a significantly high phone bill, then it is highly likely you have caught the Toll Fraud too late and the damage has been done, however you are still expect to fix any security issue.

What can I do to prevent or minimise Toll Fraud?

There are many things you can do to prevent or minimise the risk of Toll Fraud, including;

- Regularly monitoring calls made through our customer portal
- Change system and server passwords on a regular basis
- Change user passwords regularly and when staff leave
- Use a variety of upper case, lower case and numeric values when creating passwords
- Educate employees & ensure voicemail PIN numbers are not set to their defaults e.g. 0000 and 1234, or Bar or restrict premium and international call destination where necessary
- Disable any Direct Inward System Access (DISA) that may be configure red, and consider restricting voicemail access to internal phones only.
- Consider restricting access to make outgoing calls outside of business hours
- Restrict the number of concurrent calls to a number your business would expect to make at any one time.
- Restrict outgoing calls to international destinations and premium rate numbers.
- Remove remote access the phone system from outside of your business, or businesses' internal network.
- Disable, suspend or do not allow outgoing calls on extensions that are not in use.
- Access to the phone system restricted.
- Have your phone system audited.

This is not an exhaustive list and if you suspect that Toll Fraud is being committed through your phone system, you should consult an expert immediately.

How to innoTel minimise the risk of Toll Fraud

- We implement strict security restrictions across all of our external and internal systems.
- System & network passwords changed on a regular and routine basis
- System logs routinely checked for unauthorised access attempts
- Firewalls and security appliances in place with strict rules
- We always ensure we're talking with the account holder, or a nominated authority to eliminate the possibility of social engineering.
- Configure hosted phone systems according to best practise security measures

What should I do if I have been a victim of Toll Fraud?

If you believe you have been a victim of Toll Fraud, you should;

- Notify innoTel immediately on 1300 736 048 with any detail you can provide. We may elect to suspend the service(s) to protect you and us;
- Identify any information related to the hacking; e.g how the system was compromised;
- Engage a phone system with expertise in security and have them review your phone system configuration; and
- Implement steps to prevent the unauthorised access from occurring again.