2 December 2013

Fraud Prevention for Hosted Voice Phone Services

The information in this Notification is provided to help you protect your business by suggesting ways to minimise hacking risks in regard to the Hosted Voice Phone (HV) Service that you are using.

PBX Hacking
VoIP uses purpose-specific hardware and software systems to make phone calls as an alternative to the traditional circuit-switched networks managed by the carriers. VoIP systems are therefore subject to the same security considerations as any other computer network. VoIP hacking frauds cause million dollar losses around the world every year.

Why are systems hacked?
Hackers fraudulently use a company's PBX system to make long distance telephone calls and make money from these calls. Hackers exploit weaknesses in the company's PBX system using different ways. Here are some examples of the ways hackers compromise phone systems:

- IP-PBX reprogrammable through Voicemail. Hackers penetrate the voicemail and then reprogram the PBX system to make international phone calls.
- Hackers use software called SIP Vicious to penetrate the internal subscriber of the PBX through a brute-force attack in order to register IP-devices remotely and use the PBX to make international calls.
- Email addresses/Computer/Mobiles are hacked in order to get the SIP details of the user.
- Internal staff disclose SIP details externally.

Which is why you are better protected if we supply the complete HV phone system
When we supply the internet, hosted voice service and equipment, which we configure, your HV system will be more secure as our programming and processes reduce the risk of external interference and fraud risk.

How to better protect your HV phone system

- If external providers are involved as for example PBX maintainer/IT manager ensure they are using secure passwords (above all for internal subscriber), the PBX is properly configured and the network is safe. When we supply equipment we configure that equipment. We are not responsible if you change the configuration of any equipment or service.
- On IP-PBXs regularly change voicemail passwords/pins.
- Block international calls if not necessary. As a default we now deactivate international calling for all Handsets unless you instruct otherwise.
- Look for heavy call volumes at nights or on weekends and public holidays.
- Avoid providing password or configuration details or access to third parties and avoid providing those details through non-secure sources.
- If you are using BYO devices (i.e. softphones on mobile or personal laptop) ensure that they are protected and you aware of the risks involved.

What we are doing to minimize the impact of Fraud

The following processes have been implemented to assist in limiting your exposure to fraud.

- High spend monitoring: Calls are mediated and rated every 30 minutes and any service that breaks the threshold will have international calls barred. An email will be sent to you to inform you about the service barring.
- Fraud trends: Certain countries are targeted the most by hackers. Based on fraud trends some international prefixes are barred by default on our platform as a safety policy (i.e. Afghanistan).

These services are on a best effort basis and we won't be held responsible for any process failure.

Please be aware that you will be required to pay any charges generated as a consequence of your system becoming compromised. It is your responsibility to secure all the services from unauthorised use and you will be charged for any calls made by the service even if those calls are deemed unusual, unreasonable, excessive or fraudulent.

Please do not hesitate to contact me if you have any questions in regard to the HV Phone Services that we supply or that we could supply to you and ways to better maintain the security of your phone service.

Regards

Richard Martyr
Managing Director
richard@nobleheart.com.au