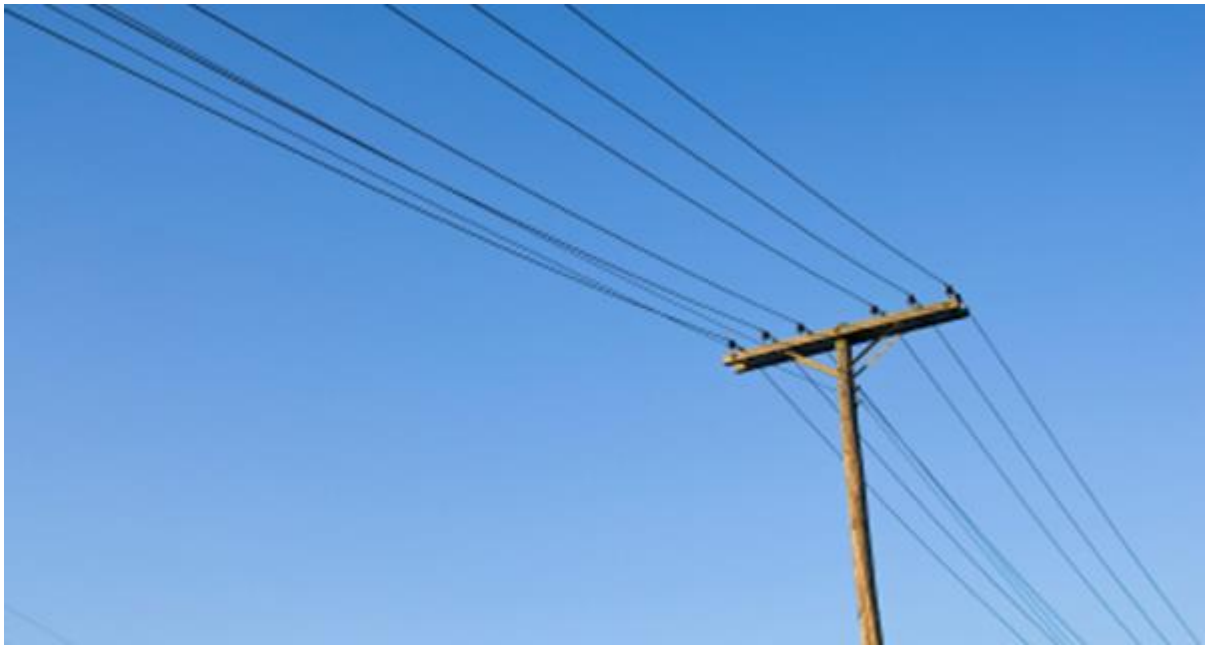
Call 0845 241 8399
Support 0871 871 8871

FIGHTING TELEPHONE/PBX FRAUD

A Guide from Voice 2 Voice Ltd



Contents

Specific types of fraud

More than 200 types of telecom fraud exist, and the methods of intrusion and theft of services are becoming evermore sophisticated. As your telecoms provider, Voice 2 Voice Ltd can help you to combat telephone fraud. This guide includes details on how to detect it – and then prevent it.

Recent scenarios

- An EU Government Authority was the victim of a telecom hack over a Bank Holiday, resulting in €300k of losses in one weekend.
- A major multinational bank lost more than $1m following DISA fraud, which had been in operation for three years before it was discovered.
- New Scotland Yard was hacked to the value of £1m over six months.
- A large advertising organisation lost £60,000 to telephone fraudsters in a four-day period.

Why?

A hacker's motive is usually simple. They do it for money, invading your telephone system to make money or to avoid paying for calls. This is achieved by:

- Selling authorised codes to organised illegal street telephone companies, who then sell illegal time on stolen network numbers.
- Stealing the codes in order to utilise the internet or simply to make illegal long distance calls.
- These activities are added to your telephone bill and can result in you being liable for thousands of Pounds worth of fraudulent calls.

Telephone hacking

Sometimes a hacker may infiltrate your telephone system to corrupt data, to take control of some of the operational aspects of the system or simply to disable it. Although this type of activity is less prevalent than the hackers' desire to simply make money, telephone hacking for malicious corporate espionage purposes should not be ruled out. Like the computer hacking world, sometimes the motivation for telephone fraud is the challenge! In this instance, access codes to the PBX are often passed to others in the hacking community, which in turn increases the risk and the cost to you.

Financial liability

Current legislation offers minimal protection against this type of criminal activity, and once your network has been infiltrated, unfortunately you are still liable for the costs. The majority of organisations decide not to report fraud for fear of negative publicity, and because it undermines consumer confidence in the security of their own services. As a result, fraud is often swept under the carpet as a `bad debt'. However, for many organisations it could be a bad debt that they simply cannot afford. The Forum of International Irregular Network Access (FINA) estimates that telecom fraud costs organisations in excess of £40 billion every year and is growing at 15% per annum.

Who is at risk?

Any organisation which has a PBX, a voicemail system, a private network or a virtual private network (VPN) is at risk of telephone hacking, regardless of its size. The PBX is one of the most susceptible areas, with typical methods of fraudulent abuse involving the misuse of common PBX functions such as Direct Inward System Access (DISA), looping, call forwarding, voicemail and auto attendant features. Frequent fraudulent exploitation is also often initiated via the maintenance port of a PBX. And with more recent technological advancements like 3G and VoIP, there are even more opportunities for hackers to infiltrate your voice network.

Telephone fraud can very easily go undetected. Like any element of your infrastructure, the telephone system needs security – as the financial and operational costs which result from huge unexpected telephone bills or inoperable systems are infinite.

<u>Telephone Fraud</u>

Without diligent and immediate attention, your telecoms system is in danger of becoming the weakest link in the network and will effectively become defenceless against targeted attacks by hackers. Almost all hackers can be deterred by the common-sense policies outlined in this guide.

Telecom fraud prevention basically falls into the categories of staff education, formalised policies on telephone security, centralised administration, greater

usage of the security features offered by your telephone system technology and last, but my no means least, increased vigilance.

Precautions

- Only enable facilities that are necessary for your telecoms needs and deactivate all system features which are not required, as the default setting.
- Change default system passwords and access codes immediately after installation.
- Bar international and premium rate service (PRS) access as standard with managed 'opt in' where needed.
- Review new or additional telecoms products to ensure that they do not compromise security in any way.
- Always treat user guides, system administration manuals and internal telephone lists as confidential material. The job of the fraudster is made easier if they can get their hands on such material.
- Review security settings and procedures regularly. Most manufacturers have developed security features but it is up to individual organisations to ensure that these features are maximised. Your system maintainer or supplier will be pleased to advise you how to get the best out of the security features on your system.
- Ensure that facilities like automatic answering or messaging equipment) do not compromise security, if they are installed on your system or extensions thereof. This includes ensuring that dial tone cannot be obtained during or following each activation or use for example, 'breaking out' of an auto attendant script.
- Review all in-house call monitoring if this facility is available. Alternatively, review itemised telephone bills and investigate suspicious call activity.
- Ensure a management policy is in place and communicated accordingly, and make sure that you follow up on any breaches of the policy.
- Educate employees on the need for security and on what they can do to help.

Specific types of fraud

1. Call forwarding

This is a feature on many PBXs and allows users to forward calls to numbers outside your organisation, which poses a huge potential security risk. For example, anyone with access to your building would be able to divert a telephone extension to, for example, Australia. By dialling that extension, their call would be connected to Australia but they would only pay for the first leg of the call into the PBX, whilst the second leg would be billed to you. So if extensions are unmanned for a period of time, the costs could be significant before the fraud is noticed.

Precautions

- Unless needed, deactivate call forwarding to external numbers.
- If practical, restrict call forwarding to normal working hours only.
- Ensure that telephone extensions that are unlikely to be used for long periods are disabled on the PBX.
- If out of hours diversion of all calls is needed, consider using the service provider's exchange facilities rather than the PBX to divert calls – e.g. utilising time plans. Many operators now offer this service.

2. Direct Inward System Access (DISA)

Hackers use a variety of techniques to gain access to your telephone equipment and systems. This includes entry via the PBX and voice messaging systems, with the most common point of entry being through DISA. This is facility which most PBXs have, but which people rarely use or even know exists.

DISA is available on many systems, allowing callers into your PBX to onward dial to destinations outside your organisation. However, as with call forwarding, you would pay the cost of the second call leg. This means that a call could be placed to any international destination for the price of the call into your PBX – and if you offer FreeCall or Freephone access, the fraudster will even get the call for free!

DISA facilities are often present but not enabled on the PBX, in fact most PBXs have DISA turned off so employees or hackers cannot access it. However, if DISA is enabled, it may be may be set up to be used with or without security

measures in place. Many companies do not understand the system and so do not activate this security feature. As a result, hackers could dial into the telephone system and make international calls at your expense. However, applications are available which can enable you to use the facility without exposing your organisation to hackers.

Hackers will often make thousands of speculative calls before they find a organisation that they can hack into. Unless you are vigilant and look out for the warning signs, you may never know whether or not your organisation is, or has been, the victim of telephone hacking.

Precautions

- If DISA is not part of your telephony requirements, ensure that it is not enabled on your PBX.
- Should DISA be a requirement, consider barring international access or selectively barring destinations which are not normally needed.
- Always protect DISA with Personal Identification Number (PIN) codes.
- If possible, have two access stages (and hence codes) to gain dial tone.
- Avoid using tones from the PBX to prompt for PIN entry. These are easily recognised by the fraudster's computer hacking programme.
- If your PBX has the facility, disconnect calls that use more than three attempts to access PINs.
- If unique PINs can be assigned, it may be possible to bar call attempts from PINs already in use, or to cease the call in progress if a second call attempt is made. This will make the service unattractive to fraudsters.
- Extend the ring delay on the PBX. Many hacking programmes will cease access attempts after two or three rings. If auto answer is delayed to four or five rings, this should help to discourage hacking attempts.

3. Remote access

On a maintenance dialup modem, logins and passwords which are not activated are generally set to well-known default values, or are not changed frequently. This leaves the door open for hackers, who could be located anywhere in the world. Hackers can remotely access and reconfigure your PBX, modifying security and dialling parameters, and designing a plan to dial in and out of the system, then returning when it is least expected.

Those who maintain or administer telephone systems usually have enhanced access privileges. However, it is possible that such access might also be gained by fraudsters, which may result in a host of functions being enabled, leading to high levels of illicit calls or even system damage.

Precautions

- Verify access to modem ports if they are within your control. Otherwise, ensure appropriate controls are in place with your system maintainer.
- Only provide appropriate access privileges to those who need them.
- Regularly change maintenance and administration passwords at least every three months, more frequently if possible.
- Change passwords immediately if an employee with privileged access leaves the organisation, or if your system maintainer is changed.
- Ensure passwords are difficult to guess or work out. For example, they should not contain your organisation name or the employee's name or be derived from readily available information.
- Maintain an audit trail of maintenance and administration activity, and review this regularly.
- If remote access ports are provided for system maintenance, consider dial back modems as a security measure.
- Remote access telephone numbers should not be easy to guess. Better still, if they are outside of the publicised number range for your organisation, perhaps beginning with different numbers, this will help to protect against hacking.
- Ask your system provider to ensure that its passwords are protected in line with your organisation's passwords.

4. Voicemail

If a mailbox password is guessable – e.g. the same as the extension number and the system is not tightly programmed, a hacker may be able to re-program the background database and the operator number in order to obtain international access.

Precautions

- PINs should never be easy to guess. For example, disallow PINs that run sequentially (123456, 654321) or the same digits (111111, 555555) or a date of birth as these are usually attempted first by fraudsters.

- Advise your staff never discuss their PIN with anyone, other than a legitimate user.
- Make it a policy for all mailbox users to record a personal greeting and to change it regularly. This will help to quickly identify any which have been seized.
- Ensure that staff delete messages after they have listened to them. If they are left to pile up they use space on the system and leave more potentially sensitive information for an intruder to listen to.
- If staff members do not use or no longer require a voicemail service, ensure that they are cancelled immediately.
- Advise your staff to report any suspicious messages to your IT department, and tell them not to erase the message.
- Unless needed, bar any function that allows access from the voice messaging system to dial tone.
- Surplus mailboxes should be locked until they are assigned to users.

5. Internal misuse

Employees are spending more and more time making personal calls, which not only results in lost productivity, but also in cost to your organisation for the call itself. The volume of non-business related calls to expensive long distance numbers, mobile numbers or premium rate numbers – made during office hours and after – is growing to unacceptable proportions.

Precautions

- Implement a reasonable 'personal calls' policy and ensure that all staff are full aware of what is and is not acceptable.
- Implement in-house call monitoring functions to identify highest cost calls, out of hours calls, calls to premium rate numbers, users with excessively high call spend and so on.
- Remember to review these reports regularly, or even better, set up alerts which will let you know if certain thresholds are breached.

6. Assumed identity

Fraudsters may attempt to call a person within your organisation, then make an excuse and ask to be transferred back to the operator. The operator then sees the call as internal and may be persuaded to give dial tone or to help with dialling an international number. The fraudster may also try to assume the identity of someone within your organisation in order to obtain an outside line. Alternatively, techniques may be attempted to gain access codes and PINs from your staff, perhaps under the guise of a telecoms engineer or similar. These codes will then be used in order to make fraudulent calls. To avoid these types of occurrences, it is vital that you educate your staff about the threat of telephone hacking, and about these types of fraudulent attempts.

Precautions

- Educate your switchboard operators and your employees about these types of fraud attempts.
- Ensure that the caller's identity is reasonably confirmed before international calls are made.
- Engineers should never request PINs or passwords. If there is a need for such information, requests should be channelled through a designated person within your organisation, who can validate and coordinate the request.
- Do not give sensitive information out over the telephone in response to a call. Always call the person back to reduce the risk of unauthorised disclosure.
- Do not connect callers to modem ports unless their legitimacy is confirmed.

What's the answer?

All of the precautions outlined above will help you to detect or avoid telephone fraud. But how can you deal with high-volume organised scams, which often rely on the exploitation of some recently found technological loophole? What is needed is a means of continuously looking for unusual calls and in particular for patterns of calls – and immediately drawing attention to them. You can then take instant action to stop a fraud as it is happening, as well as being informed about longer-term changes that may be required.

To be effective, this 'alerting' system must be able to gather details as soon as

possible after suspicious calls have been made, and then to run a flexible set of tests to check for possible fraud, whilst also estimating the cost of these calls.

Having said that, fraud identification is not quite as simple as just looking for high cost calls, and there are many other characteristics that may be suspicious in a given situation. For example, for a company that only normally trades in one or two EU countries, having anything more than perhaps three calls in a day to other countries could be regarded as suspicious. It must therefore be possible to set specific rules which are appropriate for your individual organisation.

Call monitoring and management

A call monitoring solution will interpret information from all areas of your phone system and will supply this in a series of convenient reports. These can then be reviewed and will rapidly uncover fraudulent activity. However, some forms of low-level fraud or serious internal misuse may only found by looking through reports of activity over extended periods.

The combination of an efficient call monitoring and management system, coupled with good organisational governance, will ensure that you can remain vigilant and will be able to identify fraud as soon as possible after it occurs.

In addition to this type of ongoing reporting, a good call monitoring and management system will also be able to issue alerts when it identifies situations which break the agreed rules. For example, an excessive amount of international calls, or out of hours calls to premium rate numbers.

In this way you can be kept informed about possible fraudulent activity as soon as it occurs, in a manner which you choose – e.g. email, text message or onscreen alert. Once suspicious calls are discovered, these alerts can be communicated quickly and efficiently, 24 hours a day and should then be acted upon immediately.

Advice from OFTEL

As the management of both large and small private communications systems becomes more complex, PTOs, manufacturers, suppliers and users all have a role to play in ensuring that security is maintained.

Users have the ultimate responsibility to purchase communication resources which meet their organisation's requirements, and to ensure that no unauthorised use takes place, by actively managing the resource. The UK regulatory environment permits maximum flexibility in the design and use of communications facilities, however this freedom requires the exercise of responsibility, and the principal of 'caveat emptor' (buyer aware) applies.

As such, it is the duty of all manufacturers and suppliers to make sure that users are provided with the necessary guidance and information to use and manage their communication systems securely.

Useful Links

National Fraud and Cyber Crime Reporting Centre:

PBX Dial through fraud alert:

Additional advice to consumers and the impact this is having in the UK for business'

http://www.actionfraud.police.uk/pbx-dial-through-fraud-alert-dec13

Fraudsters hacking into phone lines and making premium rate calls costing organisations millions

http://www.actionfraud.police.uk/fraudsters-hacking-into-phone-lines-and-making-premium-rate-calls-costing-organisations-millions-jul14

PBX Fraud Alert message sent 26/04/2016 14:52:00

https://www.actionfraudalert.co.uk/da/144518

PROTECT YOURSELF AGAINST PBX FRAUD

http://www.ersourocu.org.uk/64/section.aspx/58/protect_yourself_against_pbx_fraud