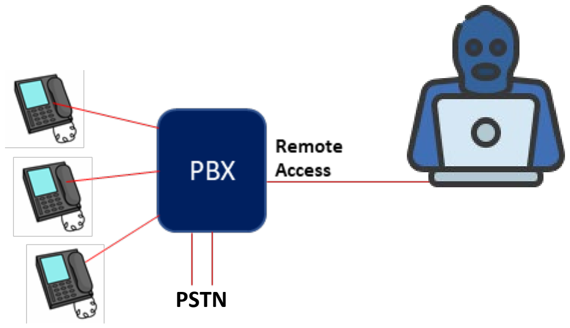
PBX Hacking – ComReg advice to PBX Owners

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation



What is a PBX?

A PBX (private branch exchange) is a telephone system to manage an organisation's phone calls. PBX owners include businesses, offices and schools. A PBX is made up of hardware and software that connects to communication devices such as telephones, hubs, switches, routers, etc. The PBX may be in the organisation's premises, or it may be a virtual PBX hosted by a communications company. The PBX owner is responsible for the security of PBX's on premises .

What is a PBX Hacking?

Hackers, located anywhere in the world, access a PBX usually through an unprotected remote access such as:

1. a number on the PBX which is intended for use by the PBX maintainer or administrator,
2. services provided by the PBX, for example voicemail.

The Hacker forces the PBX to make international calls, the PBX owner will be billed for these calls.

How can PBX Hacking generate profits?

A hacker takes advantage of telephone calls transiting through a chain of several International Networks. Each transit carries a handling charge which is paid by the network handing over the call to the next network in the chain. Hackers normally dial countries that are the most expensive but seldom called destinations, because the margins are higher than frequently called destinations. The capability to detect and regulate fraudulent calls varies across countries. This may influence a hackers call destination. The revenues will be paid between the international networks but ultimately it is the caller who bears the cost. Hackers can use call generating and call answering equipment to make multiple short duration calls to escape detection and maximise revenue.

How will you know if your PBX has been hacked?

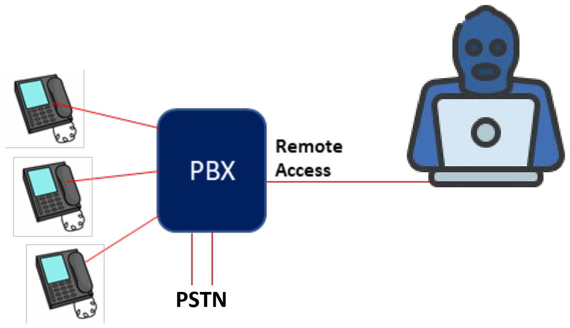
Telecommunications providers are aware of the problem and have implemented procedures to identify suspect international call patterns. These patterns are normally identifiable as repeated short duration calls to international destinations seldom called from Ireland. When telecommunications operators identify suspect call patterns, they normally block international calls from that PBX immediately and notify the PBX owner as soon as possible.

How can a PBX owner minimise the risk of a Hacking Incident?

1. Ensure all remote access circuits have strong password protection, including voicemail access. Be sure to change passwords regularly.
2. Use an approved PBX provider / maintainer. Confirm that they have implemented adequate password protection on their remote access to the PBX.
3. Disable or restrict access to countries that staff don't need to contact. The vast majority of hacked calls are made to destinations that are seldom called from Ireland.
4. Ensure that all security recommendations from your PBX supplier are followed.

PBX Hacking – ComReg advice to PBX Owners

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation



What should a PBX Owner do when notified of a Hacking Incident?

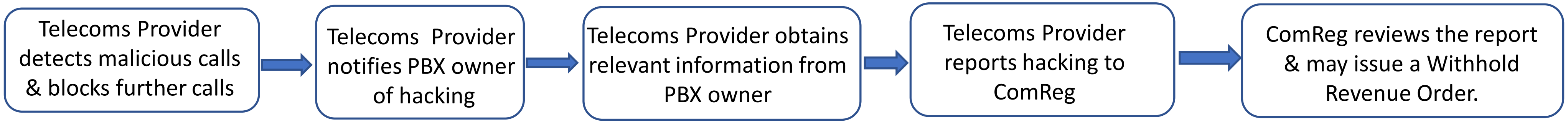
1. When notified by your telecommunications provider of a hacking incident it is advisable to follow their directions and help them to limit the impact of the incident.
2. Hacking is a criminal offence so report the incident immediately to the Gardai and obtain a Garda Pulse Number (a number allocated to the reporting of the incident).
3. Provide the information below to your telecommunications provider as soon as possible. Delays can prevent ComReg intervention
   - End User Details
   - PBX details
   - Garda Pulse Number
4. Contact your PBX maintainer for a security review.

What can ComReg do?

When requested by a telecommunications provider, ComReg can review a hacking incident with the objective of protecting end users where appropriate and proportionate. ComReg can, under Regulation 83(2) of the European Union Electronic Regulations Code Regulations 2022 (S.I. 444 of 2022), authorise an Irish based telecommunications provider to withhold relevant revenues to its onward telecommunications provider if the calls are the result of fraud or misuse of numbers. ComReg uses this authority with discretion. Where the telecommunications provider promptly provides details concerning the incident, ComReg may intervene. We will take into account factors such as the value of the calls, whether appropriate security measures were in place to prevent the hacking, and whether the incident was reported to the Gardai. If ComReg intervenes, it can mean a significant reduction in the call charges billed to the PBX owner.

ComReg will only intervene on the first hacking incident and when the Garda report has been confirmed and Pulse number provided.

How does ComReg become involved?



Telecoms Provider detects malicious calls & blocks further calls → Telecoms Provider notifies PBX owner of hacking → Telecoms Provider obtains relevant information from PBX owner → Telecoms Provider reports hacking to ComReg → ComReg reviews the report & may issue a Withhold Revenue Order.

ComReg can only stop revenue flows from hacked calls if it receives the required information before bills are paid by any operator in the chain of handling the call. It is important that PBX owners work together with their telecom's provider. Further information is available at the following link. https://www.comreg.ie/industry/electronic-communications/compliance-enforcement/misuse/