# ***PBX Security Best Practice - I3 Forum general recommendations***

This document outlines some of the most common IP PBX hacking situations and proposes some basic safeguard configurations.

## 1. Why is securing your voice switch/PBX/Gateway and following best practice rules important?

- If your network is not secure, you assume the risk of criminals seizing and sending traffic via your voice switches without your knowledge
- IP fraud is most common on weekends, special holidays and evenings when staff are off-duty
- Open source platforms/networks/switches are a core target as well as known bugs for some vendors. Keep your software updated with the latest patches.
- Fraudsters are sophisticated, organized and should not be underestimated. Given the high profit potential, they tend to be well funded and have access to the latest software tools and best programmers

## 2. Recommended actions to fulfil

- Limit PSTN dialing to essential destinations you really need to call and only ask to open those countries/breakouts
- Avoid routing plans which facilitate loop access to the PSTN via the PBX. In the case where it is necessary for contingency/backup access, check out credentials prior to access.

  Check invoicing and routing when backup mode is triggered.

  Disable remote dial-in, when possible, and dial-through capabilities.
- Secure remote maintenance ports and use call back modems or alphanumeric passwords. Make sure system administration and port numbers are randomly selected
- Enable call admission control for simultaneous call, max sessions, registration

policies, authentication for registers and authentication calls (INVITES).

- Use IPSec, TLS, & SRTP for encryption when connecting through Internet

  If downloading templates for a Centrex device is needed make sure the downloading profile is secured with https, SCP, or other secured protocol as all the users and passwords are contained in that file

  For web portals access over Internet, encrypt communications with a challenge/response authentication and a strong cypher algorithm

  Resolve DNS FQDNs with the least amount of information about your network as possible.

- Disable ports not in used. Allow only trusted VOIP IPs to send traffic to you.
- Apply patches and upgrades on a regular basis. Check regularly with your supplier for any security advisory requiring patching.
- Use some mechanism to check long term call duration and audit them based on logs
- Be aware of signs of PBX fraud such as:

  - Repeated calls of short duration

  - High numbers of incoming hung up calls

  - Unexpected increases of incoming calls where the caller hangs up when answered

  - Sudden increase of Toll Free usage or high cost destinations

  - Changing in afterhours calling patterns

- Enable dynamic dialing rules if possible, so time of day routing and routing destination policies and barring at certain times (weekends, nights, in general, out of your traffic regular patterns)
- Secure the edge with an SBC to protect your infrastructure
- Limit access and call processing to known and trusted IP addresses
- Change default password for all your servers- especially for accounts with admin privileges
- Don´t allow to use default short codes or FACs configured in the server to

change call forwards, call transfers, etc.

- Use strong password policy with a combination or capital and lowercase letters, numbers and symbols

  Do not use predictable PIN numbers, such as your extension number or public number or last digits, predictable passwords with sequential or incremental numbers, like 1234 or 1111

- Set up a password expiration policy

- Establish account lockup policies to combat brute-force and dictionary-based attack

  All these rules should be applied to all the web server management account, as well as voice access/PBX and voice mail server

  Establish proper and secure notification policies for lockup accounts

- Block all lower TCP ports (lower than 1024) to public IPs

- If ports must be accessible by Internet change the default port number using a customized one

- Block ICMP responses for critical devices

- Understand the device you are running, as some of them may allow endpoint registration only with extension and no authentication challenge, like username/ password. MAC based challenge is not recommended as it´s a weak challenge.

- Block administration access from public IP for VOIP devices

- If public access is required, implement strong passwords and only allow trusted IP access.

- Ensure these polices are also applied to voice mail portal

- Require carrier authentication for every conference call and PINS of at least a 6 digits long code, change on a regular basis

- Scan and audit your network from an IP public address, on a regular basis, to check open ports or possible security breaches

  Test your security measurements and log information by trying to access your own network from an IP public address.

Send voice call to your own network to test its vulnerability

- Ignore and block completely messages from unknown IPs. Make a silent drop so as not to provide information about your network or servers
- Never divulge system information, unless you know to whom you are giving it
- Analyze call detail activity daily (usage of CDRs).

  Use antivirus and use firewalls.
- Customers may need to take additional measurements depending on the type of platform/server/pbx in use.