Hacking is a rampant malice and any device or website on static ip is bound to get hacked someday.

It is a well known fact that criminals and hackers are always a step ahead of the authorities and we are no exception. Even the most secure data and websites are known to get hacked and are being hacked continuously as you read this. So we recommend the following precautions-

- When connecting on static ip, consider whitelisting of IP's when connecting to resources with ISD facility

- Hacking is generally aimed at making ISD calls only and to expensive revenue sharing numbers, so it is strongly recommended to deactivate ISD facility on all trunk resources connected to the IPPBX

- For ISD it is advisable to either use VOIP with prepaid or GSM with prepaid with limited access.
- As Telecom service providers have the habit of dynamically activating ISD facility, we strongly recommend taking an undertaking from them that avoids responsibility on you for such events in the future.

Final note

- Though we have taken adequate steps to block suspicious ip addresses from accessing our servers, no such precaution can be foolproof.

- When terminating any trunk with ISD on static ip in any server and not only ours it is worthwhile to engage with a knowledgeable person to get complete clarity

- A secure and well administered network is a hacker's nightmare and providing a secure network is the scope of customer and we can only have a proactive advisory role in it.