appia the cloud at work®

Tips for Preventing Fraud for Premise-Based Phone Systems

Fraudulent calling is in the news. With hackers sending unauthorized calls over phone systems, companies and organizations incur millions of dollars in expense.

What Hackers Do

Many if not most phone systems today are connected to the internet. Hackers send traffic to the internet addresses of those systems and then use sophisticated techniques to gain access to the phone systems at those addresses. It’s then a simple matter for them to send calls—calls they charge their customers for and that are free to the hackers…but not to the phone system owner.

Steps You Can Take

Here are steps you can take to reduce the likelihood of fraudulent calls. Please be sure to check with your phone system vendor or dealer for additional actions you can take with your specific phone system.

- Set your phone system so that it accepts connections only from on-site phones and specific IP addresses.
- Use strong passwords and MD5 authentication or public/private keys.
- Set passwords to eight characters in length, with at least one capital letter, at least one number, and at least one of these special characters (if allowed by your phone system): ! @ # | $ % ^ & * ( ) _ - ? .
- Configure SIP proxies and firewalls with access lists to prevent access from unauthorized IP address blocks.
- Change usernames and passwords for connected devices when a user leaves or becomes de-authorized.
- Change passwords routinely on remote connected accounts.
- Review call records regularly to be sure that traffic is what is expected from normal business use.
- Check with your insurance provider to make sure you will be covered in the event of fraud.
- Do not share SIP account passwords and device configuration passwords with anyone.
- Do not allow external users to redial from the phone system.
- Do not allow external access to the management portal of the phone system.
- Secure other services on the phone system. HTTP, FTP, and SSH are commonly exploited and should be tightly restricted.
- Phone systems should be behind firewalls, and SIP proxy services should be used to pass traffic between external and internal systems.