



## ***TELECOM FRAUD & SECURITY CHECKLIST***

- TOLL RESTRICTION:*** International locations are the major destination for toll fraud call, so toll restrict accordingly. We recommend that you start by barring all international numbers then enable only those you need to dial. Restrict outbound calling after hours.
  
- PASSWORDS:*** Change user and administration passwords frequently. Change system passwords when key personal with password knowledge leave your organization.
  
- UNUSED MAILBOXES & PHONES:*** When employees leave the company, immediately remove them all systems.
  
- EXTERNAL TRANSFER:*** Restrict call forward and call transfer features. Program your system so that extensions can forward only to known numbers and restrict all others.
  
- SOFTWARE PATCHES:*** Make sure that your phone and voice mail system has all the current software patches installed.
  
- MONITORING:*** Monitor calling patterns using call detail recording or call accounting software. Most toll fraud is generated in a short time – days to weeks and usually after hours when detection is least likely. Encourage employees to report strange language on voice messages, especially those left after hours.
  
- CARRIER FRAUD PREVENTION:*** Contact your local and long distance carrier and confirm that they have toll fraud monitoring services in place on your account. All good carriers have toll fraud measures in place.
  
- SOCIAL ENGINEERING:*** Instruct employees to never give out technical information about your systems to unknown callers, even if they do say that they are with “the phone company”.
  
- FORMAL AUDIT:*** Consider utilizing Teledynamic’s Fraud & Security Audit services, free for Telecare Priority One customers at a reduced price for Guardian One customers and available to non-support plan customers for a fee.



## ***IP PBX SECURITY CHECKLIST***

IP PBX's are susceptible to the same fraud issues as traditional systems, plus they are subject to the security gaps in your data network.

***GENERAL SECURITY:*** Develop policies, maintain strong physical security, follow best practices for securing an IP-based service, monitor resources for new vulnerabilities, maintain patches, and review logs. Consider utilizing standards-based security add-ons (TLS and SRTP) where possible.

***SECURE THE NETWORK:*** Consider using VLAN's to separate voice and data. Segmentation will greatly improve the capability to deploy pro-active defenses while minimizing the potential impact of compromised systems.

***UNTRUSTED NETWORKS:*** Use VPN's for all traffic traveling over an untrusted network.

***SECURE THE IP PBX:*** Control administrative access, user host-based intrusion prevention, and use network firewalls/intrusion prevention systems.

***ENCRYPTION:*** Consider IPsec at the IP level and/or secure RTP at the transport level.

***SECURE IP PHONES:*** Confirm firmware upgrades are current. Device authentication prevents rogue phones from registering onto the network and placing unauthorized calls.

***FIREWALLS:*** Stateful firewalls are recommended for network-level protection.

***INTRUSION DETECTION SYSTEMS:*** Intrusion detection technologies can be tuned specifically to detect IP voice threats.

***INTRUSION PREVENTION SYSTEMS:*** Intrusion prevention systems have the capability to mitigate "day 0" attacks.

***SUMMARY:*** Building security into a VOIP system is primarily about building good data security and applying it to the voice portion of the network. It's your decision to determine the level of security that meets your budget and that is appropriate for your organization. The proper security for a 10 person office is substantially different than an office with hundreds of employees.