PBX SECURITY: IT’S YOUR BUSINESS

PBX (Private Branch Exchange) Security

A PBX is a private switch that serves extensions in a business and provides access to the public switched network. If the PBX system is not maintained and secured, it can be an easy target for those with a mind to commit toll fraud.

PBX and Voice Mail Security Tips

- Run periodic security audits to check for loopholes in the PBX (have PBX vendor do this if possible).
- Disable DISA (Direct Inward System Access) if possible. If not possible, use maximum number of digits for DISA code.
- Eliminate remote access to your PBX and disable access system. Have authorized personnel use calling cards instead, if practical.
- Do not allow unlimited attempts to enter system. Program PBX to terminate access after third invalid attempt.
- Shred directories or anything listing PBX access numbers.
- Never divulge system information unless you know to whom you are giving it.
- Secure remote maintenance port and use call back modem or alphanumeric passwords.
- Tailor access to the PBX to conform to business needs.
- Eliminate trunk to trunk transfer capability.
- Restrict 0+, 0- and 10-10-XXX dialing out of PBX.
- Restrict all calls to 900, 976, 950 and 411.
- Restrict 1+ dialing to extent possible.
- Change passwords frequently.
- Delete/change all default passwords.
- Analyze call detail activity daily (use SMDRs).
- Consider allowing only attendant-assisted international calling.
- Employ class-of-service screening to areas to which there is no business need to call.

- Restrict Toll Free dialing from areas where there is no business requirement.
- Frequently audit and change all active codes.
- Deactivate unassigned voice mailboxes and DISA codes.
- Do not allow phone lines to be “forwarded” to off-premises numbers.
- Make sure that system administration and maintenance port phone numbers are randomly selected, unlisted and that they deviate from normal sequence of other business numbers.
- Use random generation and maximum length for authorization codes.
- Deactivate all unassigned authorization codes.
- Use multiple levels of security on maintenance ports (if available).
- Do not allow generic or group authorization codes.
- Ensure that “Night Bell” or attendant service does not default to dial tone when left unattended.
- Do not use “alpha” passwords that spell common words or names.
- Immediately deactivate passwords and authorization codes to known terminated employees.
- Consider implementing a barrier code system, i.e. an additional numeric password that adds a second level of security.
- Restrict all possible means of out-dial (through-dial) capability in your voice mail system.
- Frequently change default codes/passwords on voice mailboxes.

AT&T Business Services – Global Fraud Management Organization (ABS-GFMO)
24X7 Fraud Operations Center: 800-821-8235

NOTE: THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR AT&T BUSINESS CUSTOMERS AND IS FOR EDUCATIONAL PURPOSES ONLY. THERE ARE NO GUARANTEES MADE WITH RESPECT TO ITS ABILITY TO PREVENT PBX FRAUD OR ASSUME LIABILITY ON THE PART OF AT&T.