PBX and VOICE MAIL SECURITY TIPS

A PBX (Private Branch Exchange) is a private switch that serves extensions in a business and provides access to the public switched telephone network. Similarly, a voice mail system allows users to record, store, retrieve, and forward voice messages. If the PBX and/or voice mail system is not properly maintained and secured, they can become easy targets for those intending to commit fraud.

SECURITY TIPS

Listed below are a number of tips for maintaining and securing your PBX and Voice Mail systems. This list is not exhaustive and is provided for your convenience. Contact your PBX or Voice Mail systems vendor for more information.

□ Frequently change default codes/passwords on voice mailboxes.
□ 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 the system. Program the PBX to terminate access after the 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.
□ Restrict after-hours calling capability: DISA, International, Caribbean and Toll calls.
□ Analyze call detail activity daily (use SMDRs).
□ Consider allowing only attendant-assisted international calling
□ Employ class-of-service screening to areas to where 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-premise 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.

Note: The information contained herein is for **NineStar Connect** customers and is for educational purposes only. There are no guarantees with respect to its ability to prevent fraud or assume liability on the part of **NineStar Connect**