



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

<input type="checkbox"/> Run periodic security audits to check for loopholes in the PBX (have PBX vendor do this if possible)	<input type="checkbox"/> Restrict Toll Free dialing from areas where there is no business requirement.
<input type="checkbox"/> Disable DISA (<i>Direct Inward System Access</i>) if possible. If not possible, use maximum number of digits for DISA code.	<input type="checkbox"/> Frequently audit and change all active codes.
<input type="checkbox"/> Eliminate remote access to your PBX and disable access system. Have authorized personnel use calling cards instead, if practical.	<input type="checkbox"/> Deactivate unassigned voice mailboxes and DISA codes.
<input type="checkbox"/> Do not allow unlimited attempts to enter system. Program PBX to terminate access after third invalid attempt.	<input type="checkbox"/> Do not allow phone lines to be "forwarded" to off-premises numbers.
<input type="checkbox"/> Shred directories or anything listing PBX access numbers.	<input type="checkbox"/> 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.
<input type="checkbox"/> Never divulge system information unless you know to whom you are giving it.	<input type="checkbox"/> Use random generation and maximum length for authorization codes.
<input type="checkbox"/> Secure remote maintenance port and use call back modem or alphanumeric passwords.	<input type="checkbox"/> Deactivate all unassigned authorization codes.
<input type="checkbox"/> Tailor access to the PBX to conform to business needs.	<input type="checkbox"/> Use multiple levels of security on maintenance ports (if available).
<input type="checkbox"/> Eliminate trunk to trunk transfer capability.	<input type="checkbox"/> Do not allow generic or group authorization codes.
<input type="checkbox"/> Restrict 0+, 0- and 10-10-XXX dialing out of PBX.	<input type="checkbox"/> Ensure that "Night Bell" or attendant service does not default to dial tone when left unattended.
<input type="checkbox"/> Restrict all calls to 900, 976, 950 and 411.	<input type="checkbox"/> Do not use "alpha" passwords that spell common words or names.
<input type="checkbox"/> Restrict 1+ dialing to extent possible.	<input type="checkbox"/> Immediately deactivate passwords and authorization codes to known terminated employees.
<input type="checkbox"/> Change passwords frequently.	<input type="checkbox"/> Consider implementing a <i>barrier code system</i> , i.e. an additional numeric password that adds a second level of security.
<input type="checkbox"/> Delete/change all default passwords.	<input type="checkbox"/> Restrict all possible means of out-dial (through-dial) capability in your voice mail system.
<input type="checkbox"/> Restrict after-hours calling capability: DISA, International, Caribbean and Toll calls.	<input type="checkbox"/> Frequently change default codes/passwords on voice mailboxes.
<input type="checkbox"/> Analyze call detail activity daily (use SMDRs).	
<input type="checkbox"/> Consider allowing only attendant-assisted international calling.	
<input type="checkbox"/> Employ class-of-service screening to areas to which there is no business need to call.	

More information about AT&T's NetPROTECT Family of Services may be found at: http://www.att.com/business_billing/fd_fraud2.html. You may also contact your AT&T account representative or the AT&T Service Establishment Group at 1-800-NET-SAFE.

**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.