Vol. 4 No. 2
February 2012

BUSINESS insights

5 Steps that Help Protect your Business from Toll Fraud

You know about the dangers of having your business computer network hacked. The risks are high. So you install firewalls and virus protection software and take many other measures to secure your valuable business data.

Your computer network is not the only system in your business that is at risk. Your telephone system could be vulnerable to toll fraud. Toll fraud typically involves hackers accessing your connection and using it to make thousands of dollars of international calls -- which end up being charged to your business.

The 2011 Worldwide Telecom Fraud Survey revealed that, in the U.S. alone, $4.96 billion was lost due to compromised PBX/voice mail systems.

Here's what just one of those defrauded companies reported:

"We recently had our system hacked. In 2 days there were $15,000 in international calls placed. The hacker got in through the automated attendant and into an unprotected voice mail box that still had the default password."

Protecting your phone system is just as vital as protecting your computer network. Hackers look for a system manufacturer with which they are familiar, enter the system through a variety of areas and use it undetected.

There are steps you can take that can make your system a less inviting target. Here are five you can implement yourself as part of your system set-up.

1. Set up strict password rules: Change your voice mail passwords on a regular basis. Do not allow the use of passwords composed of common words or names. Make sure all passwords are six digits or longer, that they are random and that they are not related to the actual phone number. Immediately change passwords and authentication codes after any employee leaves your company.
2. Control transfers: Do not allow trunk-to-trunk transfers. Allow internal system voice mail transfers only.
3. Limit access: Limit 1+ dialing and make sure that all international calls require a live attendant to place them. Set up your system so your telephones cannot be forwarded to any off-premise phone numbers. Also, block calls to 976, 950 and 411 numbers.
4. Eliminate common vulnerabilities: Make sure there are no unassigned authorization codes in your system and remove any generic or group codes. Deactivate any unassigned voice mail boxes. Remote administration ports are a welcome-sign to hackers. Prevent the ability to forward phones to be accessed from outside the system.
5. Set up alerts: Program voice mail boxes to shut down after three incorrect password attempts. Then have the system generate an alert to you or your system administrator whenever this happens. Also, set your system up to alert you or your system administrator whenever any unused mail box is activated or re-activated.

These five steps should help prevent the high cost of Toll Fraud. Please feel free to call us to conduct a full assessment of your telecom system to determine if there are other vulnerable areas that can be made more secure.

IDEACOM® NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org