TelcoWorks

Tips for Protecting Your Firm’s Phone System from Hackers

Valerie Brauckman, President of TelcoWorks

Due to the recent increase of hacking attacks and security breaches, it is more important than ever to safeguard your firm’s premise-based and hosted PBX phone systems. Fraudulent long distance charges, caused by a PBX hack, can equate to thousands of dollars. And, long distance carriers are not required to waive the cost of those fraudulent calls. The following steps can be effective in protecting your firm from phone hackers:

— Change the system passwords once the equipment has been installed.

— If you don’t need the DISA feature, disable it.

— Use a ‘real time’ monitoring system that can alert you to unusual activity. Some security companies now offer products that will create a profile of your normal telephone use and send out an alarm when there is a derivation from that profile.

— Limit unsuccessful log on attempts to three tries.

— Use a minimum of four digits in all passwords.

— Consider insurance. Premiums can be reduced through discounts for safeguards or if other crime lines are purchased.

— Protect your RMATs if your vendor has remote access into your system.

— Deactivate unused voice mail boxes. If you are going on an extended holiday, have someone monitor your voice mail. Thieves can take over a mailbox that has a message indicating the user is not available for an extended time.

— Restrict access to problem area codes. Many companies block out area code 809 (the Caribbean). Approximately 60% of all PBX fraud calls terminate in the 809 area code. Others block out all international access codes. Keep in mind that Puerto Rico is not considered international so you will have to be specific. Emerging former East bloc countries are also a terminating point for many fraud calls. Consider your need to call these areas. Or block International calling completely.

— Limit trunk to trunk access on your systems. Some voice mail systems can give you an outside line.

— Utilize SMDR reports to detect unusual activity. Consider a security package that creates a user profile that will alert you to unusual activity.

— Limit the capabilities of your system during non-business hours.

— Make sure you have employee dishonesty insurance. An estimated 20% to 35% of fraudulent calls can be traced back to dishonest employees. Most of all, do not give up. The only thing limiting high-tech crooks is their imagination. Do not make it easy for them.

TelcoWorks is an independent voice, data and cloud consulting firm helping businesses improve their technology landscape since 2001. For more information about securing your premise PBX or hosted PBX services, call Valerie Brauckman at 610-942-7501, or go to their website at www.telcoworks.com . TelcoWorks is an ALA Bronze sponsor, Philadelphia Chamber of Commerce Technology Connector Company and a Growth Investor of the Chester County Economic Development Council.