AlternateAccess®
intelligent business phone systems

Alternate Access Quarterly Newsletter

Volume 10, Issue 2 April—June 2010

In This Issue

Holiday Closing

Alternate Access will be closed on Monday, May 31 in observance of Memorial Day.

If you need support during this time, please contact us at 919.831.4260.

Five Tips for Maintaining a Secure Phone System

We've all heard horror stories about hackers gaining access to confidential information on business computer networks. Less publicized are the stories about hackers accessing business phone systems – racking up hundreds or thousands of dollars in long distance or international phone calls on your company's tab. Business owners may not even realize that their system has been hacked until a bill arrives.

Each company should decide on the best security and password policies for their users and business.

(Continued on page two…)

Nonprofit Realizes 100% Improvement in Customer Service with VoIP Phone System

For more than three decades, Wake County nonprofit Wake Enterprises has assisted adults with severe developmental disabilities to achieve a maximum level of independence via work-related training or supported job placement in the community. The dedicated staff must constantly find ways to improve service while reducing operational costs – no small feat during a down economy.

WAKE ENTERPRISES

Most recently, the Wake Enterprises administrative staff recognized an urgent need to improve their communications infrastructure. Two locations with incompatible communications systems created a negative perception of customer service and reduced employee productivity.

The nonprofit capitalized on an office move to make the improvements, which included a strategic switch to a VoIP phone system. They discussed their needs in detail with Alternate Access and purchased a Fonality trixbox® VoIP phone system. Since the installation, Wake Enterprises has realized many benefits of the trixbox® system, including a 100 percent improvement in customer service perception. Read their entire story on our website at www.AlternateAccess.com. Just click on the Resources tab and select Case Studies.

Spring Clean Your Server Area!

With a few weeks of Spring remaining, it's not too late to complete some spring cleaning – even at the office. Make sure you add a thorough cleaning of your server area to your "to do" list.

In fact, if you haven't done so already, now is a great time to establish a server maintenance plan to ensure your server remains in top running condition year-round. There are several steps you can take to achieve this goal.

Chances are you periodically dust and sweep your home to avoid an accumulation of dust and allergens. Well, the area surrounding your server requires the same upkeep. Accumulated dust can clog air vents and coat internal cooling fans, causing servers to short out or overheat. Periodically dust and sweep the area surrounding the server to prevent such an issue from occurring.

After you've cleaned the server area, check the temperature and humidity in that area as well. Servers should be located in a cool, dry place to help combat overheating and corrosion. Make sure the temperature is constant and there is no moisture.

While spring cleaning at home, you may check and replace batteries in critical safety appliances, such as the smoke detector. Similarly, when spring cleaning at the office you should check your backup power supplies. April showers may have brought May flowers, but summer will certainly bring unexpected storms. When severe weather events pop up, they can wreak havoc on electrical systems.

(Continued on page two…)

(Five Tips continued…)

These five tips will provide a starting point for creating a security plan to best protect your phone system.

1. Do Not Give Out Your Password
It may seem like common sense, but scam artists can be convincing. One of the most frequent scams occurs via a phone call from someone claiming to be with a phone system provider. The caller asks for the system password, and then uses it to access the system and place outbound long distance or international calls.

Don't become the next victim of toll fraud. If you receive such a call, tell the caller you are not authorized to provide that information over the phone. Report the incident to your system administrator immediately.

2. Analyze Password Security Periodically
Implement a routine system security audit to expose any passwords that do not meet security standards. Some VoIP systems provide a built-in tool to automatically check for unsecure aspects within your phone system.

3. Create Stronger Passwords
In 99 percent of toll fraud cases, unauthorized access is gained through unsecure (easy-to-guess) passwords, such as ones that contain your extension number, consecutive digits (1234) or repeating digits (5555). Select a password that is easy for you to remember but not easy for others to guess. By creating stronger passwords, you can dramatically increase the security of your phone system against toll fraud.

4. Implement Company-wide Password Rules
Enforce strict password rules, instituting a minimum password length or forbidding certain digit strings like the ones just mentioned. Generally speaking, four to six digits is an optimal length for your password – long enough to challenge a hacker and short enough for you to remember. For consistency, it is wise to set a standard length in your company for all employees to follow. Another layer of security can be added by locking out a user after a certain number of failed login attempts. Your system administrator would then have to reset the user's password.

5. Change Passwords Regularly
Safeguard voicemail boxes from unauthorized access by changing passwords regularly. Your system administrator may be able to configure your security settings so that passwords expire at regular intervals (usually weeks or months).

Remember, if someone contacts you claiming to be from one of your vendors and requests your password - DO NOT GIVE IT TO THEM. Hang up the phone and immediately report the incident. If you have given your password, contact your administrator immediately so they can alert your co-workers and take the appropriate action to safeguard the system.

Instances of phone system hacking do occur, but business owners can take measures, like the ones listed above, to create a more secure phone system and deter would-be hackers.

(Clean Server continued…)

The use of Uninterruptible Power Supplies (UPS) is standard in most offices, but they must be properly cared for to guarantee they'll do the job. Alternate Access recommends that you test each UPS every few months, and replace them about every 4 years.

Schedule a recurring event on your Outlook calendar to remind you to test each UPS regularly. Mark the date of purchase on each unit using a label or marker so the "replacement date" can be easily identified. Click here to learn more about maintaining backup battery supplies.

Don't limit your spring cleaning rituals to your home. Begin a spring cleaning regimen at the office to maintain an ideal environment that

AlternateAccess®
intelligent business phone systems

5623 Duraleigh Road, Suite 111
Raleigh, NC 27612

Phone: (866) 831-9270 | Fax: (919) 831-

www.AlternateAccess.com