January 2011

TechTidbit.com

brought to you by Tech Experts

When Should Your Company Consider Adding A Server?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

If you are like most small businesses, you acquire desktop computers, phone systems, and software in a random, "buy-it-when-you-need-it" fashion as your business operations demand it.

But at some point, this patchwork of stopgap technology you've acquired needs to be examined, retooled, and perhaps replaced, depending on your company's needs.

As your business grows, it makes sense to take a broader view of your technology investments. One of the first things you might consider is the role a server would play in your company.

Servers can take on a lot of tasks for a growing business, from securing data to enabling better sharing of company resources. But it's sometimes difficult to know when, and if they're a smart investment. There are a few common scenarios in which a server can bring real benefits to a growing business - read on and see if any of these apply to you.

You need to share files, printers or other resources

It is technically possible to set up a simple network without a dedicated server, with just a few PCs connected together.

However, if you want to share databases, files, printers or other resources, a server makes it a lot easier.

In fact, servers are specifically designed for sharing, so you'll get better control, faster access, easier management and improved security. And who wouldn't want all that?

Your computers are overloaded and you need more storage

If you have a lot of files or multiple databases, it might be time to consider migrating some of these files to a server.

Whether you want to replace your old computers or just improve their performance, a server will give sluggish, data-laden PCs a welcome respite by freeing up memory and storage.

You want to have in-house company email

While businesses with only a few employees can get by with using an external service for its email, there comes a time when these services aren't ideal.

Adding a server allows you to bring your e-mail in-house, with the dual benefits of making users' e-mail access faster and keeping sensitive business information within the company - not on another company's servers. Plus, you can benefit from shared email productivity tools like Microsoft Outlook.

You want to conduct business remotely

If you have employees that work remotely, or if you'd like the option to work from home, a server will allow you and your employees to remotely access your company network, information and resources.

These are only a sampling of the signs that a server could be right for you. The bottom line is this: if you spend a lot of time moving data around, struggling to access things you need, and are worried about security, then it's time to consider a server.

> *"This patchwork of stopgap technology you've acquired needs to be examined, retooled, and perhaps replaced, depending on your company's needs."*

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Where To Report Excessive SPAM

The Federal Trade Commission, the nation's consumer protection agency, collects complaints about companies, business practices, and identity theft. You can file a complaint at: https://www.ftccomplaintassistant.gov/

SPAM Prevention FAQ: Tips To Reduce Junkmail

How can you reduce the amount of junk email you receive? Here are our best tips!

Never Allow Your Email To Be Posted Or Listed

"Spiders" and web "crawlers" routinely "harvest" email addresses from web pages in an effort to build a collection of email addresses to send junk email to.

Never Unsubscribe Or Ask To Be Removed

The only exception to this rule is if you originally signed up for that particular list or asked to receive updates.

If you never asked to be part of a participating mailing list, why would you ask to be removed? Doesn't make sense does it.

This is a common ploy spammers use to validate email addresses. If you respond, that proves to them that your email address is alive and active, and that you are receiving their emails.

Responding only encourages them to sell your email address to other spammers, and will ultimately increase the amount of junk email that you will receive.

Never Open Or Read Junk Email

Believe it or not, even if you never respond, but merely open a junk email, there could be special HTML code contained in that email message that will report back that you opened or read the message.

This provides validation to the spammer that your email address is alive and active, and you can bet you will start receiving more spam!

Be sure to turn off your email program's Preview Pane feature, as this is essentially the same thing as "reading" a message.

Avoid Contests, Special Offers, And Chances To Win

These are gimmicks to get you to reveal your email address so they can send you special offers. Many free ecards (electronic greeting cards) are also ways companies collect email addresses.

Never Post To An Email List Using Your Private Email Address

Many spammers watch these posts in order to harvest new email addresses. So be very cautious when posting to these websites.

If you are a contact for a registered domain, do not list you private email address.

Instead of using your personal email address use a generic common mailbox for this purpose, or ask for domain registration privacy.

Create a public email address such as DNS@yourdomain.com or help@yourdomain.com.

Guard Your Computer Against Trojan Spyware And Software

Never open any attachments you don't explicitly trust.

Some "fun" emails are often a ruse to steal email addresses or track your behavior on the Internet.

The use of both anti-virus, personal firewall, and or anti-spyware software is strongly recommended.

Use A Free Account As Your Public Email Address

Reserve your private email address for friends and select associates.

Never sign up for special offers using your private email address. Use your generic common email address for those.

Trick The Spammers

If you post an email address online, disguise its set-up, spelling out 'dot com' in place of .com.

Junk Mail Out Of Hand

If your junk mail has reached a level that it is just out of hand and you cannot handle it anymore, consider changing your email address.

If you don't want to change your email address consider us to take advantage of our advanced SPAM filtering services.

We can make all necessary changes on your computer and with your email service to help prevent those spam messages.

New Technologies Make Proactive Service A Must

With today's workplace relying more and more on information and computer systems, it just makes sense to leverage your IT investments.

Technology in the industry now allows IT professionals to take a proactive approach to network management, providing the entire infrastructure with a complete, secure, reliable, and fully automated solution to protect your IT infrastructure.

Deploying what are known as "agents," you can add a fully automated virtual worker to your staff, which is working 24 hours, 7 days a week, 365 days a year. This agent will complete a long list of tasks that even a fully staffed IT department couldn't handle.

You can now start to enjoy your away time when your network is being monitored by these solutions. So what exactly do they do?

Monitoring

When you use system monitoring, you can take the proactive approach to your computers and servers with a set of rules that your administrator defines.

They provide instant notifications of problems or changes such as low disk space on your hard drives, memory leaks, power problems, virus activity, and missing updates. Just about every critical component of a PC or server can be monitored.

Software Deployment

The software engines give us the ability to deploy software out to multiple systems simultaneously, which saves massive amounts of time and causes less downtime for the staff.

Given a set of rules and pre-requisites that are met prior to the install, you can ensure a smooth, fast, and worry free installation across your network.

Remote Control

Give your IT personnel a secure and quick way to remotely access your systems from any place at any time, giving your company its own help desk in a sense.

This increases productivity for staff, reducing the waiting time for a tech to show up at your location.

Patch Management

Keeping your computer systems up to date with operating system updates and security patches is critical to the health and safety of your network.

Given a set of predefined policies, all of your servers, workstations, and remote computers will automatically be receiving the latest security patches and software updates on a schedule that works for you.

Keeping the data traffic on the network during normal operation hours is crucial to the efficiency and productivity of the workplace and this will do just that.

Reporting

The reporting features will provide your administrators' with quick and easy access to all the details of a network. Tactical and strategic planning become effortless when the agents are accumulating, tracking, and analyzing the way your network operates over time.

Audit & Inventory

Agents let the IT staff perform accurate and detailed reports on every server, computer, mobile device, and piece of equipment on your network.

This gives you a better look at what your network actually consists of and provides you and/or your IT personnel a complete detailed inventory of product specifications, versions.

An accurate network and infrastucture inventory lets you make intelligent decisions about upgrades, replacements, and maintenance.

Scripting

Possibilities are practically endless for what can be done with the scripting options. If you have a routine task that has to be done each and every day, week, or month, let your agents do the work.

They can automatically trigger those tasks to be done for you, on your time, your schedule, with no interaction required.

These are just a handful of the features that are possible, giving everyone a peace of mind when it comes to your IT.

Taking advantage of these technologies will give your IT personnel a complete set of tools to efficiently, securely, and cost effectively manage your systems.

Create new service requests, check ticket status and review invoices in our client portal: https://connect.expertsmi.com/support

Contact Information

24 Hour Computer
Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(866) 993-9737
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our
client portal! Log on at:
https://connect.
expertsmi.com/support

TECH
EXPERTS

980 S. Telegraph Road
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Strong Passwords Keep Your Personal Information Secure

A recent ZoneAlarm survey revealed that 79 percent of consumers use risky password construction practices, such as including personal information and words.

The survey also revealed that 26 percent of respondents reuse the same password for important accounts such as e-mail, banking or shopping and social networking sites.

In addition, nearly 8 percent admit to copying an entire password found online in a listing of "good" passwords.

Given these numbers, it's no wonder that 29 percent of respondents had their own e-mail or social network account hacked, and that over half (52 percent) know someone who has had a similar problem.

The first step a hacker will take when attempting to break into a computer or secure account is try to guess the victim's password.

Automated programs are available to repeatedly guess passwords from a database of common words and other information.

Once a hacker gains access to one account, almost 30 percent of the time that information can be used to access other sites that contain financial data such as bank account numbers and credit card information. To ensure you stay safe online, here are a few tips for creating a strong password.

Use Unique Passwords For Each Account

Choose different and unique passwords for each account.

Passwords Should Be Eight To Ten Characters Long

Choose a password that is at least eight to 10 characters long. This should be long enough to prevent brute force attacks, which consist of trying every possible combination of a password until the right one is found.

Avoid Using Personal Information

Make sure your password is difficult for someone to guess. Do not use names of any kind, including your login name, family member's name or a pet's name. Also avoid using personal information such as a phone number, birthday or place of birth.

Avoid Words In The Dictionary

Avoid words that can be found in the dictionary. With the availability of online dictionaries, it is easy for someone to write a program to test all of the words until they find the right one.

Avoid Repeating Characters Or Sequences

Stay away from repeated characters or easy to guess sequences. For example: 77777, 12345, or abcde.

Use Numbers, Letters And Special Characters

Choose a password that is a mixture of numbers, letters and special characters. The more complex and random it is, the harder it will be to crack.

Use Word Fragments

Use fragments of words that will not be found in a dictionary. Break the word in half and put a special character in the middle.

Frequently Change Your Passwords

Change your passwords often. Even if someone cracks the system password file, the password they obtain is not likely to last long.

Cyber crime is on the rise. Taking the time to actively choose secure passwords will protect your identity, banking information and personal information. And remember, writing your password on a sticky note on your monitor isn't secure!