August 2016

TechTidbit.com

brought to you by Tech Experts

Five Ways Cloud Computing Can Improve Your Business

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

Regardless of the size of your business, you can harness the power of the same high-tech tools used by Fortune 500 companies, thanks to cloud-based technology.

According to recent studies of small- to medium-sized businesses, those using cloud computing greatly outperformed those that didn't. One study showed an average of 26% more growth and 21% more profitability for small- to medium-sized businesses using cloud computing over those that only had their heads in the clouds.

Here are five concrete ways the cloud can help your business:

Reduced costs

Cloud computing eliminates the need for a large IT department. With the data centers located off-site, your business is not responsible for the electricity to run, maintain, or periodically upgrade those servers.

The money saved by using cloud computing can then be redirected into growing your business or marketing to new clients.

Increased flexibility

Using the cloud to store and share files gives users much flexibility to choose how and where to work.

Data can be accessed from a variety of devices and from anywhere, which can greatly increase the amount of ground covered in a shorter period of time.

Better security

There's little doubt about the importance of keeping sensitive business data secure from prying eyes, but many small- and medium-sized businesses don't have the budget to beef up security substantially.

With a cloud computing service, there are built-in layers of security which is an especially attractive option to control access to business files, if you have employees or contractors that work remotely.

Storage and backup solutions

Over time, your business accumulates documents and files that gradually create an on-site data storage problem. By using the cloud to store your data, you not only eliminate the worry over available space, but also guarantee a backup in the case of a virus infestation or a major natural disaster.

Ability to grow

While a small- to medium-sized business may initially use only a handful of tech tools, there will be a greater demand for the collaboration, storage, and flexibility benefits that cloud computing provides. With cloud computing already in place, there is no need to completely restructure systems as your business scales up.

> The money saved by using cloud computing can then be redirected into growing your business or marketing to new clients.

We're proud to partner with the computer industry's leading companies:

Microsoft Partner

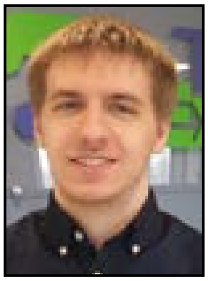
Microsoft Small Business Specialist

Business Partner IBM

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

Anti-Virus Advice For Your Small Business

> *"In a recent study, household name Symantec (Norton) was labelled with multiple critical vulnerabilities that in fact make the system less secure than if it was running without an anti-virus program."*



Brian Bronikowski is Field Network Engineer at Tech Experts.

Anti-virus has always been a major concern for users at all levels. From trojans and keylogging programs, to ransomware and malicious software, there is always a new threat on the table.

When we purchase an anti-virus software, there is a certain feeling of security we expect to have, that there is no worry when it comes to those malicious attacks. That's what the money goes towards. The problem is that sometimes anti-virus actually does quite the opposite.

In a recent study, household name Symantec (Norton) was labelled with multiple critical vulnerabilities that in fact make the system less secure than if it was running without an anti-virus program.

One would hope that a company of this size would be able to resolve these before they're discovered — or at the very least, promptly look for ways to clean up their act. Unfortunately, Symantec wanted to put on the brakes and wait before patching these flaws that affect every product associated with the company.

Most of the affected systems have been patched since the first reports from June. When you see a report like this and pair it with the performance-degrading effects large anti-virus companies impose, it becomes a simple question: what do you do?

There are a multitude of protection software on the Internet and in-store. Some of these will go back and forth in terms of highest rankings. Some are big brands that are pre-installed on most computers. Others are less well known, but gaining ground. It's all about finding the right one for you.

More often than not, we will see the likes of McAfee and Norton on systems. These are loaded for you when you buy a new system and will start as a trial. Users will often purchase the system instead of going through the arduous task of properly removing an anti-virus program.

The problem here is that generally the user will purchase whatever is "recommended" which will often be an entire security suite. These will bring a low-end computer to a halt and greatly degrade the mid-range and higher end computers.

It is important to stay away from the big names like these as there is little innovation and plenty of flaws. Some of these flaws may be performance alone and others are security flaws.

Some of the lesser known programs are often times a good alternative. With these, it's always good to look at any recent vulnerabilities or complaints users have had.

Some protection systems have deleted files or overwritten system files in the past. Research is important for these situations. That said, common free programs, such as AVG and Avast, are found on millions of systems.

Keep in mind, most free protection softwares have one catch or another. Spam-like interfaces that constantly ask for purchase or the requirement for manual scanning are the most common culprits.
If you are able to stay on top of things, these can work out well enough.

Unfortunately, most users are unable to due to the workload given to them. Protection ends up being an afterthought; one that can cost a lot more than the software itself. There is one nearly foolproof way to get rid of these worries for good: allowing professionals to take care of your protection.

Tech Experts is able to supply a managed anti-virus that is inexpensive, well-reviewed, and kept up-to-date with the latest virus definitions. We are able to install it in both home and business environments.

With that in mind, it's an easy choice when picking what you want to shield you from the dangers of the digital world.

Is It Ever A Good Idea To Share Your Password?

Luke Gruden is a Help Desk Specialist at Tech Experts.

There are times when it can be tempting to share account information or give a coworker access to files and programs to streamline processes. Other times, you might be away from the office and someone may need something on your Windows.

There are many reasons why workers would want to share accounts and passwords that would be in good faith and, on the surface, best for business. Should this be allowed and acceptable in a work setting? The short answer is no, and for several good reasons.

As much as it would seem that sharing passwords and credential information could help workers, this can lead to poor habits and huge security variabilities. All it takes is for one person to write a password down for another person to read it.

It is common for someone using social engineering to go into company buildings and look for sticky notes, note pads, or files on desktops with passwords and account information on them. This way, they have the means to steal company information.

Even worse, it will look like the user account that was used to steal information was the one stealing information instead of the thief.

Another common event at some work places is that some workers will use their coworkers account to do something risky, so if anything happens, the account holder is the one in trouble and not the person borrowing their account.

When it comes down to the pressures of keeping a job or to work towards promotions, it can be surprising what some people might resort to in achieving their goals.

Sometimes, a person sharing an account might make a mistake and mean no harm, like deleting some important files on accident or click something they didn't know about in an area of the computer they normally do not have access to. This would also look like the account holder made the mistakes and not the actual person. There is a reason why certain people have access to certain drives, websites, and programs. Permissions and restrictions should be respected.

Your Windows account and email are your unique fingerprints and they should be protected. Everything you do on a computer is recorded in event logs and possibly on other monitoring systems on the network. Your account information should serve you as well as prove the work you have done.

It may be tempting to share account information, but there are alternatives. If a coworker needs access to a program or website, let IT know.

If the coworker really needs access for their job, then your manager and IT will change permissions to allow them access and they'll no longer have to ask for your password.

What about if they need to work on files that you are working on? Your IT can setup a network drive and enable access for both you and your coworker so that files can be edited and changed freely without ever logging into each other's accounts.

There may be many other reasons as to why people may want to share their account information, but chances are, there are alternatives that your IT can implement so that no one's personal credentials are given out. Keep your account your own and there will be no unnecessary risk or possible security threat out in the open. If you have security or user concerns or would like to develop a permissions plan, we would be happy to help. Give us a call at (734) 457-5000.

> *"As much as it would seem that sharing passwords and credential information could help workers, this can lead to poor habits and huge security variabilities. All it takes is for one person to write a password down for another person to read it."*

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

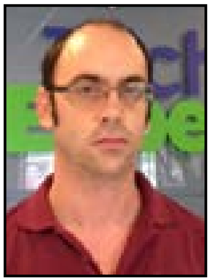
Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Guest WiFi: Improves Security And Customer Satisfaction



Mike Simonelli is a Senior Network Technician at Tech Experts

One of the first things I look for when I enter any establishment is the WiFi network. My laptop needs it. My phone needs it. I need it. It comes as a shock to me in the rare circumstance that I can't find one or, worse yet, when I do find one but I am denied the network password.

Usually when this happens, I am there as a consumer. This annoyance is even more frustrating for people that are visiting for business such as vendors, consultants, and clientele.

Such people rely on Internet access to communicate with their own offices via e-mail and instant messaging or remote access to product databases and other information.

These frustrations can be avoided by the addition of a guest WiFi network and can even benefit your own existing WiFi network. Adding a guest network to an existing WiFi infrastructure can be a cost effective way to improve the overall security and privacy of your network.

Segregating your network will keep your workstations, servers, printers, and other network devices secure while keeping your clients, vendors, and other guests off your main network. Allowing visitors unrestricted access to your company's primary WiFi network can be a costly mistake. These unmanaged mobile devices can carry all types of sophisticated malware, trojans, viruses, and network probes, just waiting for a chance to attack your network.

Keeping these devices segregated to their own guest network will, at the least, add a layer of protection to your own equipment.

Not only will a guest network keep visitors off your primary WiFi, but it will also keep you from having to give out your primary network's password to a multitude of strangers. A complex, never changing password can be used for your employees, while a short and simple password can be given out to guests upon arrival, and then changed frequently.

In addition, you can configure your equipment to only broadcast the network ID of your guest network and keep your primary network ID a secret, adding an additional layer of security.

Finally, some of the higher-end WiFi access points and routers will allow you to limit the amount of bandwidth that is allocated to your guest network or control the type of traffic that is allowed to pass through it. Doing so will prevent your visitors from inadvertently bringing your network to a halt with bandwidth-hogging traffic such as streaming video and torrent downloads.

If your business is already allowing visitors access to the primary WiFi network, then there is simply no downside to configuring a second WiFi network for guests, especially if your wireless hardware already supports the option.

Doing so will make your network more secure by allowing you to keep the network IDs and passwords a secret, as well as make it easier for your visitors to connect. Once connected, your guests can then be limited as to how much of your resources they can use, ensuring that your normal business operations aren't interrupted.

If you have any questions about WiFi permissions or how you can increase both security and customer satisfaction in one go, contact us today by calling (734) 457-5000.

Create new service requests, check ticket status, and review invoices in our client portal: *http://www.TechSupportRequest.com*