March 2016

TechTidbit.com

brought to you by Tech Experts

Improve Your Staff's Productivity Using These Five Tips

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

Increasing employee productivity is a positive approach for companies, regardless of the industry; however, the concept can be rather vague.

Productivity means more than just working to meet a given quality standard, therefore, it isn't always immediately clear how to achieve optimum outcomes while maintaining standards and keeping your employees happy.

Here are a few concrete methods that can help your staff be more productive:

Block certain Internet sites

With the rise of social media, online gaming, video sites, gaming and contest portals, and entertainment websites, there are many potential distractions on the web.

Even if an employee is well-intentioned, there are plenty of well-designed trappings to keep them there, wasting your company's time and, ultimately, money.

Consider placing a block on potentially productivity sapping sites to remove the temptation to linger online.

Try mobile app blocking

Just as employees can get distracted while on computers, they can also waste time piddling away with apps on their smartphones.

While there is no way to completely solve this problem, you can at least block the use of certain applications when connected to the corporate network with technology such as firewalls.

Revamp technology

It isn't necessary to invest a fortune in buying new equipment to upgrade your IT infrastructure and increase your staff's productivity.

Get rid of any obsolete technology that just takes up space, update your software, and consider investing in one or two pieces of newer equipment that can benefit multiple staff members or perhaps the whole company.

Save files in the company's cloud

Get rid of clutter on individual computers while promoting collaborations between members by using cloud storage.

This frees up space on each computer station for optimum speed, and you can set permissions on files to share between certain staff members while restricting access to others.

Track production

There is a wide array of tracking methods to measure how many tasks an employee undertakes during a work day.

Many industries have developed tools and established best practices to manage and track production times and quality.

If you're having trouble finding the best tools to use for your business, give us a call and we'll work with you to find the solutions that will work for you.

It isn't necessary to invest a fortune in buying new equipment to upgrade your IT infrastructure and increase your staff's productivity.

Does Your Backup Plan Stand Up To A Disaster?

"Businesses in industries of all kinds expect the worst to happen to them, and your business can't afford to be any different."

Michael Menor is Vice President of Support Services for Tech Experts.

Technology, while a great asset that can be leveraged for your benefit, can also frighten businesses due to how unpredictable it can be at times. The constant threat of data loss, identity theft, and hardware failure can cripple your business's ability to retain operations.

Specifically, businesses can learn about risk management by analyzing the processes used by an industry where risk management is absolutely critical: nuclear power plants.

In the wake of two of the most destructive and violent nuclear disasters, nuclear power plants have begun to crack down on how they approach risk management. The Chernobyl incident of 1986, as well as the tsunami-induced disaster at Fukushima in 2011, are the only nuclear disasters to reach the peak of the International Nuclear and Radiological Event Scale (INES) at a rating of 7.

This means that they had an immense impact on the immediate vicinity, as well as the environment on a worldwide scale.

The meltdown at Chernobyl was the result of an uncontrolled nuclear chain reaction, ending in an enormous explosion that resulted in fire raining from the sky and radioactive core material being ejected into the vicinity. A closer inspection of the incident revealed that the explosion could have been prevented, had the plant practiced better safety measures and risk management, like having a containment system put in place for the worst-case scenario.

In comparison, the Fukushima plant was prepared to deal with a failure of operations.

The problem that led to a disaster was one which couldn't possibly have been prevented: the 2011 Tōhoku earthquake and the resulting tsunami. The Fukushima plant had a contingency plan to shut down the plant in the event of a disaster, but tsunami prevented this from happening properly by flooding damaged power lines and backup generators, leading to heat decay, meltdowns, and major reactor damage.

Disasters like these lead to professionals searching for ways to prevent emergency situations in the future. For example, the Fukushima incident kickstarted conversations on how to prevent problems caused by the unexpected issues.

In response to emergency power generators being flooded or destroyed, off-site power generation will be implemented as soon as November 2016.

One other way that nuclear plants have chosen to approach these new risks is by outsourcing this responsibility to third-party investigators, whose sole responsibility is to manage the reliability of backup solutions. In a way, these investigators function similar to a business's outsourced IT management, limiting risk and ensuring that all operations are functioning as smoothly as possible.

What we want to emphasize to you is that businesses in industries of all kinds expect the worst to happen to them, and your business can't afford to be any different.

Taking a proactive stance on your technology maintenance is of critical importance. While your server that suffers from hardware failure might not explode and rain impending doom from the sky or expel dangerous particulates into the atmosphere, it will lead to significant downtime and increased costs.

In order to ensure that your business continues to function in the future, Tech Experts suggests that you utilize a comprehensive backup and disaster recovery (BDR) solution that minimizes downtime and data loss risk.

BDR is capable of taking several backups a day of your business's data, and sending the backups to both the cloud and a secure off-site data center for easy access.

In the event of a hardware failure or other disaster, the BDR device can act as a temporary replacement for your server. This lets your business continue to function while you implement a suitable replacement.

Small Businesses Experience Increase In DDOS Attacks

Bruce Stykemain is a Network Engineer with Tech Experts.

Some readers may already be wondering, "What exactly is DDoS and why should I worry about it?" DDoS stands for Distributed Denial of Service – and a DDoS attack is when a person (or group) acts maliciously and uses a program which has a sole purpose of flooding a server with traffic.

Why would someone do this? There are many reasons one would execute this devastating attack. For instance, you run a news website. You publish an article that this person doesn't agree with.

They, in turn, run their malicious program. It sends thousands upon thousands of page requests (unique requests to open the website), which causes more traffic than your server can handle.

Your server crashes from the load and no one is able to view your site. Of course, this could be one reason among an infinite amount. For whatever evil agenda they have, it does not fare well for those on the affected side.

In 2015 alone, there were some 50,146 attacks that were detected – averaging 137 per day and 5 per hour (Newswire, 2016).

While these attacks may not make national news or headlines, the IT world is paying close attention. With more devices and easier programs to use, almost anyone could be on the bad side of the cyber war.

One of the more recent attacks that happened was on New Year's Eve. A group calling themselves New World Hacking took down BBC's global site and Donald Trump's site. Another big attack was aimed at a big part of the Internet itself. Namely, the 13 DNS servers on the backbone of the Internet.

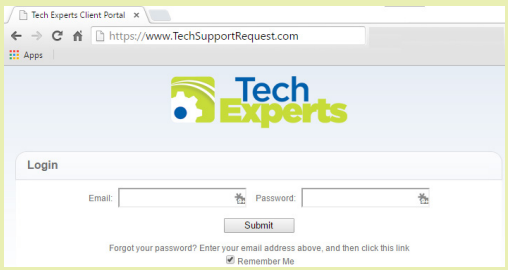
These servers are important because they translate the words we use (such as website addresses) into the numerical equivalent that the machines understand. There were two separate attempts, one being 160 minutes long and another lasting about an hour. It caused three of the DNS servers to go offline for a couple hours or so, which is enough to cause a lot of slowness issues or DNS errors on a lot of people's screens.

What can be done to help mitigate this issue? There are a few things. You definitely should have an IT department or IT security group who is able to handle this. Bigger corporations especially should be keeping up with threat trends and keeping their firewalls and security prevention up to date and active.

Now, say you're a small to medium size business and you have no security on your network. It would be a good idea to have an IT service provider such as Tech Experts to help with your IT and security needs. These days, especially in recent years, it's not a good idea to just pay your cousin under the table to install a router and call it good.

If you can't afford to have anything happen to your data or to be down for a day or more, hire a professional. We can set you up with a network designed with your needs and security in mind.

> *"While these attacks may not make national news or headlines, the IT world is paying close attention."*



Create new service requests, check ticket status, and review invoices in our client portal:

http://www.TechSupportRequest.com

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

Easy Spring Cleaning Steps For Your Computer

Just as it's a good idea to periodically clean out closets and other areas of your home as part of spring cleaning, your computer needs decluttering attention as well.

This not only makes it easier for you to find files when you need them, but can also speed up the computer performance.

Check for viruses

If you do not have an antivirus installed and set to regularly check your system, make it your first priority to install an antivirus.

Not all viruses put out obvious signals like the blue screen of death; some can lurk in the background, slowing down your computer's operations or running malware without your knowledge.

Use a disk cleaner

Disk cleaners scour your system looking for files you don't use, particularly useless temporary ones. Such files won't impact how your programs work, and they just take up valuable space and can even make your computer run slower than it should.

Organize your files

If you have long lists of files, try grouping them into folders. This will save you a lot of time when looking for something in particular and also makes your storage more aesthetically pleasing.

Toss unnecessary programs

You've likely tested out programs and decided they weren't for you or even grown tired of them. There's no reason to keep them. Go into your Control Panel and select Programs to see everything that's on your computer.

Uninstall the ones you can readily identify as ones you no longer want or need, and leave the ones you don't recognize alone in case they are important. Check and uninstall any web toolbars, too.

Delete your web history and cookies

Over time, all the little data records of where you've been while surfing the web accrue, and can greatly slow the functioning of your computer.

Deleting your web history, including cookies, is something you should not be doing just during spring cleaning, but on a regular basis to keep your computer operating at optimum speed.

Severe Security Vulnerabilities Patched by Microsoft

Early last month, Microsoft released 13 security patches as part of Patch Tuesday.

While such security measures are usual, this one was particularly important because six of those patches were categorized as critical and require user attention to be put into place.

These six patches addressed programming flaws that had the potential to give cyber-attackers the means to gain full user rights in a wide array of Microsoft's software programs. The remaining seven patches address the elevation of privileges, denial of service, and ways to bypass security features.

The programs that were at risk from these flaws included all supported versions of Microsoft Windows, the new Edge browser, Internet Explorer, Microsoft Office (including Services and Web Apps), Microsoft Server Software, Adobe Flash Player, and Microsoft .NET Framework.

According to Microsoft, these flaws were detected before any actual security breaches stemming from these issues actually occurred.

If they had not been discovered, cybercriminals may have been able to gain user rights to Microsoft programs via specially crafted websites from remote locations.

Microsoft strongly urges Windows Vista and later operating system users to ensure the latest updates have been installed, especially if they do not have their systems set for Automatic Updates.