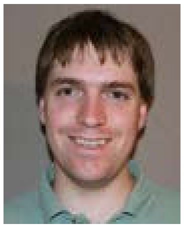
TechSolutions INC.
Managed Services
Computer Consulting
Network Administration
TechPoints

# Two Promotions Here at TechSolutions

We are happy to announce that we have promoted Patrick MacBride and Chris Scerbo to the position of Advanced Network Technician. Patrick started with us 5 years ago as a PC Technician II and since has passed rigorous exams in order to achieve the certification of Microsoft Certified IT Professional – Server Administrator. His responsibilities include managing, maintaining and troubleshooting clients' computer networks. He is a native Delawarean who resides in Pike Creek along with his wife, son and daughter and is a member of the American Home Brewers Association.



Chris graduated from the University of Maine and joined TechSolutions 4 years ago as a PC Technician II after moving to Delaware. His responsibilities include network administration and application development. Working with computers since the age of 10, he has achieved A+, Network+ and Cisco certifications as well as Microsoft Server certifications in Windows Server 2008, Exchange and SQL technologies. He possesses a strong background in programming and web development. He lives with his wife and daughter in New Castle and likes to make noise on the holidays by putting on fireworks displays as a licensed fireworks technician.

TechSolutions' president, Rick Monnig, said both team members have exhibited what we like to call the 'can-do' attitude by continually upgrading their skill levels and doing what it takes to meet the needs of our clients. They have demonstrated advanced troubleshooting skills that make them more than qualified for the position. We congratulate them on this achievement and are pleased that our clients will benefit from the expertise they bring to the table.

BACK TO TOP

# Computer Malware! What happens now?

*Signs that you have an infection and tips on avoiding one*

By Chris Rule, PC Technician II
TechSolutions, Inc.

It's the last thing you want to see on your computer, a message claiming your PC is infected with scary sounding applications. It's something we see every day here at TechSolutions, but when you're not sure what to do or what is happening, it can be a frightening situation.

In recent months, we have seen an upswing in malware infections, particularly a version that installs what looks to be an official security alert informing you that your PC is rife with all types of malware. The virus announces you're infected and then locks down your internet connection and disables your anti-virus or anti-malware software to prevent you from removing it. But this is all a ruse, an attempt to gain your credit card information by having the virus claim the only way to remove the infection is to purchase their anti-malware solutions over the internet using your credit card.

While many times it's obvious when you have a malware infection, sometimes it is not. Some behaviors to look for would be:

- Sudden slowness on the PC that doesn't have a legitimate explanation.
- Having a large amount of pop up messages while on the internet.
- Suddenly being unable to access internet or network resources when you had access before.
- Unusual or never before seen messages from your PC claiming that you have a malware or virus infection.

If you suspect your computer has been infected, the first thing to do is take a deep breath, relax and call the TechSolutions help desk at 302-656-8324. DO NOT click on, or follow the suggestions of any virus messages and attempt to remove it by using or buying their application. It will not work, and will probably infect you with more malware. It almost certainly isn't as bad as it seems and chances are good it can be fixed. Any malware can be removed with the right tools, knowledge and time. We employ a variety of solutions that have been shown to be effective at removing malware infections including rootkits that hide even deeper in a PC's file system. **Our goal is to strike a balance between effectively removing a malware infection while also trying to get your PC back up and running in a time efficient manner.** Additionally, we test most of the commercially available anti-malware and anti-virus applications and use only the ones we find most effective. When you call us to remove a malware infection for you, you can be assured we have a vast amount of experience in dealing with these issues and will do our best to remove what ails your PC.

Many of our clients have asked us what can be done to prevent or eliminate a virus or malware infection. Unfortunately, there is no magic bullet. These types of infections happen in a variety of ways, and new ways are always being discovered and exploited. However, there are some common sense steps you can take to minimize the chances of your PC becoming infected.

> First, ensure you have an anti-malware application installed on your PC and it is updated regularly. We recommend a centrally managed antivirus solution for all business networks. As an alternative for home users, we have found Microsoft Security Essentials to be a good, free, anti-malware solution (Free download on http://www.microsoft.com ). Call us for more details on whether your business has a proper anti-malware software package.
>
> Second, minimize unnecessary web surfing on your work PC. Even if you know and

trust a website, it is possible to get an infection by merely visiting a compromised website. Additionally, use caution when clicking on links contained within emails or on social networking sites. Before clicking, ensure the link goes where it purports to take you by placing your mouse over the hyperlink and viewing the text. The resulting pop-up should somehow correlate to the intended website.

Third, refrain from opening files or documents that you can’t be sure are safe. Avoid opening files from people you don’t know or don’t know why they would have sent you something. Certainly there is no way to be absolutely sure, but if it seems suspicious, recreational, or unnecessary for work purposes, it is probably better to avoid opening it.

Fourth, refrain from installing programs or applications on your PC that aren’t necessary for work. Many programs install applications that open connections on the internet to report usage data, error messages, and check for updates. While usually harmless and legitimate, this does expose your PC to possible malware infections.

Lastly, do not store any business data on your local hard drive, but rather on a network drive that is backed up nightly. Home users should ensure that critical data is backed up regularly. While this has nothing to do with getting a malware infection, it’s good to have backup data in case the malware infection compromises your PC so much that the data is either destroyed or can’t be recovered.

In conclusion, while none of us here at TechSolutions wants to hear that any of our clients are infected with malware, we’re prepared with the tools, expertise and staff to assist you in removing malware in an efficient and thorough manner. Don’t delay in calling us if it happens to you.

BACK TO TOP

# Who Goes There? Understanding Multi-Factor Authentication

*With an assist from Facebook*

A bedrock element of IT security involves granting and restricting access. When we think of access, we generally think of user names, PINs, and passwords -- the mainstays of identity authentication in the information age. We use them all the time throughout the course of the day: accessing our devices, networks, local applications, and cloud apps.

For people who spend a lot of time thinking about information security, things like passwords, user names, and security questions constitute one type (one factor) of authentication. Namely, these are all things the user *knows.*

The federal government recognizes three distinct authentication factors: things you *know* (passwords, answers to security questions), things you *have* (keys, swipe card), and things you *are* (i.e., physical traits such as eye color, fingerprints). Adding a second factor offers a significant jump in security. A third factor -- facial recognition or iris scan, for example -- offers an even greater deterrent against unauthorized access. Military and intelligence agency networks are often guarded by three-factor authentication.

For a network or application to qualify as having "multi-factor authentication," the user must be required to clear two out of three authentication factors.

There's a lot of confusion about what qualifies as multi-factor authentication and what doesn't. For example, if you're required to type seven passwords to access an application, there's still only one factor of authentication between you and the app -- that's because those passwords are all things you *know.*

Now to Facebook. Recently, the social network rolled out a multi-factor authentication process, which it calls "log-in approval." When a Facebook user tries to access her account from an unrecognized computer, Facebook sends a unique, one-time code via text message to her mobile device. She then inputs the validation code and is granted access to the social network.

At first blush, this looks a lot like single factor authentication. The code is another bit of information the user knows, right? The difference is that the user must have his cell phone in order to receive the randomly-generated code. With two out of three factors, Facebook's "log-in approval" scheme meets the multi-factor standard.

We'll conclude with a question for you to ponder: Would you feel more secure or less secure if Facebook rolled out three-factor authentication? :)

BACK TO TOP

# A Worrywart's Guide to Cloud Computing

*Can the cloud be trusted? Yes, but you still have to do your homework!*

The public cloud represents a utility model of computing: you pay for what you use, scaling up or down as needed, without having to worry about back-end stuff like installing updates and keeping server racks cool.

But giving up the burdens of management also means giving up the comforts of control. How can you be sure your cloud provider has your best interests at heart? Will they take steps to ensure the safety of your data?

According to research from the Ponemon Institute, the majority of cloud providers (69 percent) believe security is primarily the responsibility of the cloud user. A mere 16 percent of cloud providers say security is a shared responsibility.

In other words, you're right to be worried. But not too worried. Worry, in the correct dosage, is a good thing, because it leads to smarter decisions. In excess, it gets in the way of opportunity.

So don't let security concerns paralyze you. The cloud is a wonderful thing, and if you're scared of the above statistics, you shouldn't be, because cloud providers are right: security is your responsibility, no one else's. (So is finding quality vendors, many of whom are seeking a competitive advantage by offering comprehensive security to their clients. Hint, hint.)

As an aside, we predict most cloud vendors won't be so blasé about security for very long, once the adoption of cloud computing plateaus, with a lot of small and mid-size businesses (SMBs) waiting for cloud providers to get serious about security.

The larger point we wish to make is that you can never assume security. You must research, trust (and then verify) when you choose a public or private cloud provider, or take steps on your own end to mitigate your risk. In an ideal scenario, you'll do all of the above.

This makes finding a cloud computing vendor a lot like finding any other vendor when sensitive information is involved. For example, if you're looking for payroll services, do you take steps to ensure the trustworthiness of the service provider who will be handling your employees' personal information, including social security numbers and bank account numbers? Of course you do! The same kind of due diligence -- no more, no less -- is required when moving IT apps or parts of your infrastructure to the cloud.

Speaking of due diligence, here's a list of suggested criteria when considering a cloud vendor:

**Evaluating a prospective cloud provider**
Key metrics for measuring overall trustworthiness:

- Years in business
- Datacenter locations
- Customer reviews (online, firsthand)
- SAS70 certification
- BBB accreditation/compliant history
- Customer service (accessibility, reliability)
- Secure socket layer (SSL) protection?
- Privacy policy - Clear and fair?
- Terms of service - Clear and fair?
- Vertical-specific considerations: HIPAA, PCI DSS compliance

If you need assistance or have specific questions, we're happy to work with you and evaluate the solutions that are right for your business needs. Also, we can help you explore available options (including hybrid-cloud solutions) that can keep your business going in the right direction. Contact us with any questions you may have!

BACK TO TOP

# The Case for Summer Vacation

*Science says breaks are good for you*

We tend to think of leisure as a luxury. A knock to productivity. A borderline un-American activity.

Owners of small businesses are particularly susceptible to this line of thinking. According to Payscale, the average U.S. small business owner takes less than 1.5 weeks of vacation each year. Owners with 1-9 years of experience log only 0.9 weeks of vacation annually.

This is very, very bad.

The hardworking men and women at our nation's small businesses NEED to take more time off, if only to ensure more years of productivity. Consider the following statistics, published in Intuit's "Small Business Owner's Guide to Taking a Vacation": men who take vacations are 32 percent less likely to die from heart attack; women who don't take vacations are up to 8 times more likely to suffer from heart disease.

That's right, ladies and gentlemen: Vacation is no laughing matter - it's a matter of life and death.

Vacation is necessary because it offers a blend of **rest** and **play**, both of which are essential to good mental and physical health. What's more, rest and play are high-yield investments in your productivity: vacationers report a 82 percent increase in job performance when they return to work, according to Payscale.

> **"The opposite of play is not work, it's depression."**
> **- Dr. Stuart Brown**

If you want a scientific case for taking a play-filled vacation, we suggest watching this presentation by Dr. Stuart Brown, a neuroscience researcher whose insights on play come from studying animals, drunk drivers, and murderers -- seriously.

Brown's breakthrough came when he discovered a common thread among convicted killers: a lack of play in early childhood. With years of research behind him, Brown can now point to a strong correlation between overall success and playful activity -- in childhood *AND* adulthood.

"The thing that's unique about our species is that we're designed to play through our whole lifetime," says Brown. "We are the most plastic of all creatures, and therefore the most playful, and this gives us a leg up on adaptability."

We're not saying you'll become a homicidal alcoholic if you don't take summer vacation this year, but you might become a tad surlier than you would otherwise. What's more, you might miss out on some good ideas: vacation offers a beneficial distance that can help you solve vexing work problems and generate cool new ideas. There's even a neuro-scientific basis to this phenomenon. According to Brown, "Nothing lights up the brain like play."

» See also: The Small Business Owner's Guide to Taking a Vacation

BACK TO TOP

# Video Offers Terrifying Look at the Stuxnet Worm

Discovered in June 2010, the Stuxnet computer worm gained global renown when it was implicated in the disabling of Iranian centrifuges used for uranium enrichment (prompting Iran to issue an RFP to counter-hackers). Stuxnet is considered more complicated and more potent than any other virus on record. Though it seems to have focused its destructive capability on Iran's nuclear program, dormant copies of the worm were found on scores of other networks around the world, including some that controlled pressure gauges for nuclear reactors. Stuxnet covered its tracks by telling system operators that everything was normal. But wait, it gets worse...

» Watch the video

BACK TO TOP

[redacted]