FEBRUARY 2015

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

The Smarter Path

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Willie Kerns, SmartPath Technologies

What's Inside:

(270)238-8997

Fill the Backpack Helping local schools

The BackPack Food Program discreetly provides low-income students with packs of nutritious, child-friendly food items to take home on weekends and school breaks so they can return on Monday ready to learn.

During the month of February, SmartPath Technologies will be collecting food and donations to be given to the local schools.

If you would like to help out just drop your food or donation at our office. If you would like a list of items needed please email carol@smartpathtech.com.

Is Anything In Life Really FREE?

***Warning:* If You've Downloaded Free Software From The Internet, Your Computer May Be At Risk For Viruses, Hackers, and Spyware!**

We've all heard the saying that the best things in life are free, but I'm not sure they were referring to software.

Freeware (free software, not to be confused with open source software) such as the AVG anti-virus free edition, Spybot, and Ad-Aware are all programs you can download to your PC for the ultimate discount: free. However, you get what you pay for.

While these programs may work just fine for someone's home computer, they are not business class tools and should not be trusted to completely protect your computer or network from viruses, spyware, hackers, and other problems.

Every month we receive calls from clients whose computers are infected with a nasty virus or a boatload of spyware who had these programs installed and running, and were under the false assumption that they were protected.

Why Freeware Doesn't Protect Your Computer

In most cases, freeware is a light version of a software program that you pay for. Take the AVG free edition for example. AVG offers a free edition of their licensed product as a way of introducing you to their fully-featured product. However, this software does not come with any online, e-mail, or phone support. It is also illegal to use it on multiple machines or in a commercial, non-profit, or educational environment (single home users only).

You're On Your Own

As you might expect, freeware comes with zero guarantees or promises to function correctly, to be compatible with your system, or to safeguard you from threats. You're not a paying customer so you're on your own to resolve any technical problems you encounter, and you certainly won't get support if your computer gets infected.

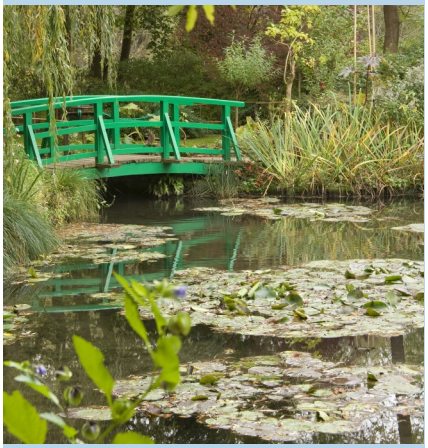
Since many free applications are plagued with bugs and incompatibilities, you may end up with a mess on your hands and no one to blame but yourself.

Additionally, freeware programs are not always current with the most up-to-date protection, and don't always update themselves automatically or perform scans and tasks on a regular schedule. That means you could be operating with a false sense of security; and since the sophistication and number of threats circulating are only increasing, you need a comprehensive solution that you can trust especially if your computer or network holds data and files you don't want to lose or make available to a cyber-criminal.

Bottom line: you get what you pay for. If the files, data, pictures, and functionality of your computer or network is of high-importance, then investing in a trusted, industrial-strength software program to protect it is a smart and worthwhile investment.

The Lighter Side…

Punch a Painting, Go to Jail



In 2012, Andrew Shannon punched a Monet painting valued at $10 million. The incident occurred at the National Gallery of Ireland, located in Dublin. The painting, entitled *Argenteuil Basin with a Single Sailboat*, painted in 1874, apparently represented something much greater to the man who decided to attack it.

Right after his initial arrest, Shannon said the attack represented his way of "getting back at the state." Later on, when he appeared in court, he changed his tune. Instead of an "attack against the state," he said the whole thing was just a big misunderstanding. He said he didn't punch the painting, he "fell into it." He told the court he had felt faint and fell. The painting just happened to be in his way.

Fortunately, the National Gallery has plenty of CCTV cameras and the whole thing was recorded. What did those cameras see? Andrew Shannon very deliberately thrusting his fist through the Monet painting. In December of 2014, he was sentenced to five years in prison, and *Argenteuil Basin with a Single Sailboat* is back on display after being fully restored.

"Sure, it's all fun and games until someone loses an iPhone."

Note to Parents

Growing up in the 80's, my parents had it easy. All they had to do was keep me and my three siblings alive. Now, I'm sure they will disagree considering we spent most of that time trying to kill each other. Perhaps they would even accuse us of having it easy. We don't have to worry about our kids getting bored and looking at the tops of two grain bins and wondering if they could climb up and jump the gap. Or going outside to find them jumping off the house onto an old mattress. Both are true stories, aside from some minor flesh wounds, we never got truly hurt, but I'm sure we took years away from our parents. Kids today have other ways to keep their mind occupied inside the safety or their own homes. This is certainly true in my case, then again we don't have grain bins close by. However we do have to worry about something they didn't. Online safety and social media. I'm not an expert in child behavior, but I do have enough boys to fill a basketball team and a couple of cheerleaders to cheer them on. So when asked to write an article, you write what you know.

Christmas is over and if you are like me, your kids have new tablets, game consoles, phones or other some other device that connects to the internet. I think it is important to know how to use these devised and what your kids use it for. Fortunately, kids are like sponges, they absorb everything and can pick these things up and just know how to use it. Unfortunately, kids are like sponges, everything they see or do online is also absorbed. How they use this new found knowledge will either make you proud, or put a pit in your stomach. My wife and I have always tried to stay on top of the "porn" issue with the kids, but I will admit we were slow to catch up with all the different social media sites. After running into several issues, we have been forced to catch up. How do you deal with your kid's social networking? Honestly, we don't know. We have nothing to draw from, our parents didn't have to deal with this. We did our research, and found that the most common suggestion was to talk to your kids and monitor their online presence. I'm sure this works for a lot of people, but there are a lot of social media sites and apps out there used by kids, if you multiply that by the amount of kids you have, that can quickly become a full time job.

Social Media is a great tool and makes communicating with a lot of people very simple, but it can easily be abused, even by adults. When it comes to kids, the dangers of abuse are multiplied. They can easily get caught up in the drama or fall victim to abuse by strangers. They can run the risk of meeting the wrong people or get in the middle of a heated online argument. This list goes on and I'm sure there are issues that I can't even imagine. I can't give you a sure fire way of managing these issues, but I can tell you what works for us. Talking to them is important, not just once but several times. Maybe you can reason with them and explain why it is important, or you may simply have to lay down the law. We finally decided to limit the kids to one social media site of their choosing. We have their passwords and we check it often. If there is anything posted that we don't approve of, they lose that device and the privilege of having a social media account. They can only talk to people they actually know like family or friends from school, and never post address, phone numbers, or anything (even in a private message) that you don't want your Grandma to see. We also make them turn in all devices before bed. This seems to be effective for us, but you have to find what works for you and your kids. Don't turn a blind eye to social media and don't expect it to go away.

Dr. Nido Qubein is president of High Point University, an undergraduate and graduate institution with 4,300 students from 40 countries. He has authored two dozen books and audio programs distributed worldwide. As a business leader, he is chairman of the Great Harvest Bread Company, with 220 stores in 43 states. He serves on the boards of several national organizations, including BB&T (a Fortune 500 company with $185 billion in assets), the La-Z-Boy Corporation (one of the largest and most recognized furniture brands worldwide) and Dots Stores (a chain of fashion boutiques with more than 400 locations across the country). As a professional speaker, Dr. Qubein has received many distinctions, including the Golden Gavel Medal, induction into the International Speaker Hall of Fame and as the founder of the NSA Foundation in Arizona. To learn more about Dr. Qubein, go to: http://www.nidoqubein.com/

Shiny New Gadget of the Month

Prizm

This month's gadget is so new, it isn't even off the assembly line. Meet Prizm — a small, pyramid-shaped device designed to make your home-audio experience as hands-off as humanly possible. The device was recently backed on Kickstarter this past November. The French company behind the audio device wanted to create an intuitive music experience that brings users new music, while learning what they really love to listen to.

The device streams music from cloud services such as Deezer, Spotify and SoundCloud, with more services planned in the future. It works by accessing your WiFi network. It doesn't contain any speakers, so you'll have to supply your own (it connects via Bluetooth, 3.5 mm stereo jack and optical audio). And despite being called hands-off, the device sports buttons to let you like or skip songs to customize your listening experience.

It can currently be pre-ordered from www.meetprizm.com for $139.

Hackers & Cyber Criminals Are Concentrating Their Attacks On Small Business

"As the security becomes better at large companies, the small business begins to look more and more enticing to computer criminals," said Charles Matthews, President of the International Council for Small Business, "It's the path of least resistance."

Think your network is secure? Take a look at these surprising statistics:

⇒ One-fifth of small businesses don't have up-to-date antivirus software installed.

⇒ Sixty percent don't encrypt their wireless links.

⇒ Two-thirds of small businesses don't have a security plan in place.

⇒ Eighty-five percent of the fraud occurs in small and medium-sized businesses.

Why is security so poor for small business? Primarily for two reasons:

Ignorance. Most small businesses believe that nothing could ever happen to them, and therefore don't take the necessary precautions to secure their network, monitor their systems, and train their staff.

They are also ignorant on HOW to get this done (which makes a strong argument for getting all of our clients on our ITWorks!) The second reason is that they are **being cheap in the wrong places.** Some simply refuse to spend money on securing their network. That's akin to having a beautiful home full of expensive furnishings and valuables, but refusing to buy a good lock for the door because it "costs too much."

So what should you do at a minimum to protect your company? Here are 7 fundamentals:

1. Educate your users on security basics such as using strong passwords, and not downloading "cute" screen savers. Some companies make computer security rules part of their standard HR policies and make each employee sign that they understand the rules.
2. Install a web filtering software to police users and prevent accidental (or intentional) slip-ups on the above- mentioned usage policies.
3. Install a good virus protection system on all computers on your network and maintain it (for our ITWorks clients, we do that for you.)
4. Install a firewall and check the logs periodically (again, we manage that for our ITWorks clients.)
5. Remove all unessential services and applications installed on your servers. After e-mail, this is probably the biggest security vulnerability. If a hacker gets in, this will reduce their ability to use a forgotten service or application to exploit your network.
6. Keep all your servers updated with all the latest security patches.
7. Never keep any of the manufacturer's default settings on any of the appliances or software you install. Hackers know what these settings are and will use them to gain easy access to your network. This item nails more systems administrators than care to admit.

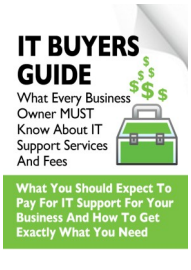
For those of you on our ITWorks Plans, you can rest assured we are taking good care of issues 3 through 7; however, if you would like us to conduct a training class and develop an AUP (acceptable use policy) for your staff and then install a content filtering software to help enforce the policies, give us a call. If your not an ITWorks client, inquire about these items today.

This training and software is a small price to pay for the peace of mind you'll have over your network's security. And since better than 80% of all security breaches happen because of an end-user mistake, you'll also be taking a big step towards protecting your assets.

FREE Report: The Business Owners' Guide To IT Support Services And Fees

You will learn:

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.



Claim Your FREE Copy Today at www.smartpathtech.com/ITbuyersguide

78 Ash St
Calvert City, KY 42029
(270) 238-8997

Are You STILL Keeping Critical Passwords On A Post-IT Note Next To Your Computer? Read On For An Easy Way To Remember Your Passwords And Maintain High Security...

One of the hardest habits we struggle to get our clients to break is writing down their passwords on sticky notes by their PC. Obviously this is a security risk. Another bad habit is choosing really easy-to-remember passwords such as “password.”

But admittedly, it CAN be hard remembering all of those darn passwords that are always changing. To solve this little dilemma, we’re suggesting to our clients to stop using passwords and use “pass-phrases.”

What is a “pass-phrase” you ask? They are letters and numbers put together in an easy-to- remember phrase such as “GoEagles09!” These are MUCH easier to remember than a random cluster of letters and numbers, which means you won’t have to write them down on a post-it note anymore!

Pass-phrases can be built from anything, such as favorite quotes, lines from movies, sports team names, a favorite athlete’s name and jersey number, kids’ names and birthdates, pets, and so on.

All you need to do is be a little creative to get numbers, letters and punctuation into the phrase. Since introducing this to our clients, we’ve found (believe it or not) they actually have fun doing this! Just don’t get so proud of your pass-phrase that you share it with others!

Examples:

L0s3w31ght? **pl@n@tr1p$** **s@v3m0n3y$**

Qu1tsm0k1ng! **W0rk0ut?** **2k1d$&1d0g**

y0ursp3ci@l! **b3h@ppy*** **B3stm0m!**