Technology Today

Brought to you by: Snap Computer Solutions LLC

AUGUST ■ 2012

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

"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!"
- Kendall Reinford, Snap Computers

What's Inside:

FREE Small Business Advisory Guide:

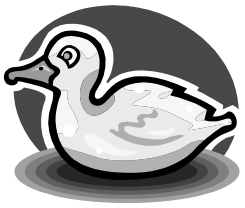
16 Critical Questions Every Small Business Owner Must Ask Before Hiring Any IT Company

At www.snapcomputers.net

If Disaster Strikes, How Fast Could You Be Back Up & Running?

You hear it all the time from us—back up your data, keep your virus protection current and install and maintain a firewall to protect yourself from hackers and other online threats. However, while these precautions will certainly help you avoid problems, they CAN'T do anything if you don't have a good backup and disaster recovery plan in place.

Are You A Sitting Duck?



We all know that an ounce of prevention is worth a pound of cure; yet, disaster recovery planning often takes a distant second to the daily deadlines and pressures of running a business. That means that most businesses, including your own, may end up offline and without important data after a simple lightning storm.

Don't think that could ever happen to you? Consider this: "data-erasing disasters" can also take the form of office fires and broken water pipes, not just earthquakes, floods and tornadoes. If a fire started in your building, the parts that weren't burned beyond recovery would probably be destroyed by the firemen's efforts. But even more common is software corruption, hardware failures and human error!

7 Disaster Recovery Questions You Need To Answer

A disaster recovery plan doesn't have to be complicated, time-consuming or expensive. Start by asking yourself the following questions…

1. Do you back up your company's data daily to both an onsite *and* offsite location?
2. Are you absolutely certain that your backup copy is valid, complete and not corrupt? How do you know for sure?
3. If disaster strikes, HOW would you get your data back, and how long would it take? In many cases it takes days and often weeks; what would you do during that period of time?
4. Do you have copies of all the software licenses and discs in a safe location that could be accessed in the event of having to rebuild your server?
5. Would you and your employees have a way to access your network remotely if you couldn't get to the office?
6. Do you store important passwords in a secure place that company officers can access if you are unavailable?
7. Do you have a UPS (uninterruptible power supply) device in place to keep your network and other critical data operations running during a power outage?

Call 717-283-4030 to schedule your Disaster Recovery Assessment so we can be sure you are ready BEFORE a disaster ever strikes.

Get More Free Tips, Tools, and Services At: www.SnapComputers.net

Shiny New Gadget Of The Month

myfitnesspal

Here we are in August…the year is more than halfway over! How have you done with your New Year's commitment to "get in shape" or "eat better and exercise more?"

Well, if you have fallen off the wagon, I have some good news for you. And even if you have stuck with it, this little tip can make your efforts even easier.

MyFitnessPal.com provides a FREE online tool for tracking your diet, exercise activity and fitness goals. This site makes it easy to set your weight loss goals and overall nutrition plan. Each day you can log in to track food you eat for a breakdown of calories, fat, carbs and protein of each item. Any exercise activity can be logged and will subtract from your daily calorie bank.

There is also a social element to this site. Much like Facebook, you can ask to "friend" other members, post on a common wall and share encouraging words throughout your journey to good health.

MyFitnessPal.com is easy to use on your computer or via apps available for iPhones and other Smartphone devices.

As they saying goes, "That which is measured improves." By simply tracking and measuring your food and exercise results on a daily basis, you become accountable for everything you eat and for every activity—or lack thereof. Seeing your progress in black and white will surely boost your results!

Check it out:
www.MyFitnessPal.com

Bring Your Own Device To Work: **Excellent Money-Saving Idea Or Security Disaster Waiting To Happen?**

There is a trend happening in business called "BYOD" (bring your own device) where employees are bringing their smartphones, tablets and other devices to work.

Considering the cost of new hardware, this trend seems pretty attractive for small business owners. Employees show up already equipped with the devices they need to work; you just give them a username and password and you're off to the races without as many out-of-pocket expenses as before. Plus, the employees are more than happy because they get to continue to use their device of choice. Cool? Maybe…

Based on surveys and chatter online from IT managers and executives, how to effectively monitor and manage employee-owned devices is murky at best; in many cases, this "wild west" device strategy is causing IT departments to work overtime to keep their network secure and data out of the wrong hands. For example, IBM started allowing employees to BYOD back in 2010. Approximately 80,000 of their 400,000 employees started using non-company owned smartphones and tablets to access internal networks. But instead of IBM saving money, this situation actually increased costs in certain areas, namely in the management and security of those devices. Because of this, IBM has established guidelines on which apps the employees can or can't use. In addition, employee-owned devices are configured so that they can be wiped remotely in case devices are stolen or misplaced prior to being granted access to internal networks. Cloud-based file-transfer programs such as iCloud, Dropbox and even Siri, the voice-activated personal assistant, are not allowed. Employees with greater access to internal applications and files will also have their smartphones equipped with additional software that performs the appropriate data encryption.

The bottom line is this: If you are going to allow employees to use their own personal devices to connect to your network, you need to make sure they aren't a conduit for viruses, hackers and thieves; after all, we ARE talking about your clients' and company's data here! That means written policies need to be in place along with 24/7 monitoring of the device to ensure that security updates are in place to watch for criminal activity. We also urge you to establish a policy for all employees who bring mobile devices into the workplace about what they can and cannot do with their devices. They might already be using their smartphone or tablet to access e-mail or company files without you even knowing it, leaving you exposed.

For more information on how we can monitor and manage ALL the devices connected to your network, give us a call: 717-283-4030

Quotable Quotes On Business

"Leadership is doing what is right when no one is watching."

– George Van Valkenburg

"The only limits are, as always, those of vision."

– James Broughton

"Your most unhappy customers are your greatest source of learning."

– Bill Gates

"It's not information overload. It's filter failure."

- Clay Shirky

"Success is a pile of failure that you are standing on."

- Dave Ramsey

"Relationships are the foundation of leadership."

- John Maxwell

What Should You Do If YOUR Network Is Compromised?

Back in June, 6.3 million passwords were reported stolen when a hacker was able to access LinkedIn's servers. The news made headlines instantly and everyone in the office (and online) was talking about it. Clearly this is a public-relations nightmare for the company and one that will, for sure, have a ripple effect for months, possibly years, as they deal with the fallout from their clients and potential lawsuits.

What's scary about this type of attack—or any major security breach to a big company—is that if it can happen to them, it can certainly happen to YOU. Although I'm not privy to LinkedIn's security procedures, I'm sure they don't take it lightly and have most likely invested a BIG chunk of change to keep their data secure, money that the "average" small business owner could never afford to logically spend. So IF this happened to your company, what should you do? How do you avoid a massive PR mess, the loss of both sales and the trust of your clients, and even potential lawsuits?

The first step would be to identify what type of attack it is and what machine (s) were affected so you can quickly contain the damage done (or being done) as best as possible and protect your assets. Naturally, you should consult with a professional security expert (like us) to make this containment happen as quickly as possible to "stop the bleeding."

Next, you'll want to notify any and all parties affected as fast as possible. In the LinkedIn attack, they immediately notified the subscribers affected by forcing a password reset. The faster you can react to this, the better your chances are of limiting the damage done. We're not legal experts here but we *would* encourage you to talk to an attorney about the breach and about what you need to do in terms of making a public announcement as quickly as possible—particularly if a security breach exposed your employees, subscribers or clients to a cyber-criminal. In some cases where medical or financial information is involved, you may be required by law to report the incident not only to your clients, but also to authorities.

Of course, you can't saw sawdust, which simply means there's nothing you can do to un-do a security attack. Beefing up security AFTER the fact is good, but a better strategy is to avoid being complacent to the point of being negligent. After all, if a security attack happens and it's due to a simple security measure you could easily have put in place, it looks really bad.

If you're a Snap Premium Support Member, you can rest easy knowing we're monitoring your network against such attacks to limit your risks and prevent you from being low-hanging fruit for hackers. If you're not a Snap Premium Support Member, call us for a FREE Networks Security Audit to see just how secure your network REALLY is, and to find out how you can hire us to take care of this for you.

5 Ways To Keep Your Laptop Running – Without Plugging It In

On the road, in the airport, at a client's site, or simply at home on the couch. These are places you can't – or don't want to – plug your laptop in. Want to keep your laptop running as long as possible without searching for an outlet? Here are 5 tips to help:

1) Keep your screen dim. A laptop's backlight requires a lot of power. Reducing the brightness conserves battery life.

2) Turn off unused hardware. Your Bluetooth and your Wi-FI receiver can both be turned off if not in use. Unplug your external mouse or other device. And mute the PC's sound system. Not only will it save power, it avoids annoying everyone else around you.

3) Don't multitask. Run as few programs as you can get away with. Stick to one application (word processor, browser, or whatever) if possible. (If online keep your antivirus and firewall on in the background.)

4) Avoid multimedia. Save your photo editing and video watching for when have AC power. These tasks suck up immense battery life. To listen to music, use your iPod (or similar device).

5) Sleep, standby or hibernate. Sleep mode (a.k.a. "standby" in XP) keeps your PC on. It still uses power, just less than normal. Hibernate uses no power initially, but a lot of battery life to start back up.

How Much Work Are Your Employees *Really* Getting Done?

Interruptions come in many forms. Phone calls, emails, faxes, colleagues, vendors. And once a person is interrupted, it can take as much as 30 minutes to get back on track. According to a recent study from the University of California, employees have an average of only 11 minutes of uninterrupted time on any given project; and they typically have 12 projects going at once. All this interruption adds up to over 10 ½ hours of unproductive time per week, says the study. So what advice does the study give to resolve this productivity loss? Close your email, let your phone go to voicemail, and shut your door – at least until the next crisis strikes.

On a Personal Note...

This past month marked 10 years since my mother passed away from cancer. It is a time of remembering the wonderful person she was and all she put into my life. She was a great example of love, patience, and kindness and I learned so much from her. I wanted to share a little glimpse of that with you. A few weeks before she died, she wrote in her journal the following important lessons that she learned in life. I hope this inspires you:

1. That life is very precious and a gift from God
2. The Word of God is powerful and effective
3. The Word of God is the Word of God
4. That God loves us more than our finite minds can understand
5. That we need to store up our treasures in Heaven--our treasures reflect our hearts
6. That eternity and knowing Jesus is all that matters
7. That Heaven is our REAL HOME. We want to long for Christ's appearing in our hearts and spirits
8. That waiting on God's timing is a blessing and a protection over our lives
9. It always pays to be honest and truthful
10. That family is your most dear and cherished treasures on earth. You take them with you to Heaven
11. To guard our hearts--it is the wellspring of life
12. To take every thought captive
13. To allow God to be the Potter in your life to prepare you for TIME and ETERNITY
14. To be fully surrendered to God and His plan for your life
15. To TRUST God--He is worthy to be trusted
16. That suffering can be a gift
17. Forgive freely
18. Look for the best in others
19. Go to bed with a clean slate
20. Pray about everything

Kendall