MC Connect

"Insider Tips to Make Your Business Run Faster, Easier, and More Profitably"

5 Cell Phone "Urban Legend" Myths Debunked

There have been a number of e-mails circling the Internet talking about hidden tricks and features of the average cell phone. Below are a few of those myths and the actual truths according to Snopes.com.

Myth #1: The emergency number worldwide for mobile phones is 112. This number can be dialed even when the keypad it locked.

Truth: Calling 112 on your cell phone will connect you with local emergency services in some parts of the world—primarily Europe—even if you are outside of your service area, and some phones will allow you to dial 112 even if you lack a SIM card or if the keypad is locked.

Myth #2: If you have a remote keyless entry system for your car and lock your keys in the car, you can call someone with a spare key and get them to transmit the "unlock" signal via your cell phone. Simply get them to press the unlock button on the spare key into their cell phone while you hold your cell phone close to the door. It will open instantly.

Truth: Cars with remote keyless entry systems cannot be unlocked by relaying a key fob transmitter signal via a cellular telephone.

Myth #3: Pressing *3370# on your cell phone will unlock hidden battery power on your phone.

Truth: This is a misunderstanding of an option available on some brands of cell phones, such as Nokia. However, this option is activated by pressing #4720#; pressing *3370# actually enables Enhanced Full Rate Codec, which provides better sound quality at the expense of a *shorter* battery life.

Myth #4: You can totally disable a stolen cell phone by giving your phone's serial number to your service provider and reporting it stolen; they can disable the phone so that even if the thief replaces the SIM card, the phone is still useless. You can get your cell phone's serial number to display on your phone by punching in * #06# on your phone keypad.

Truth: Entering the sequence *#06# may display a 15-digit identification code string, but this function only works with certain types of phones. Plus, reporting this number to your service provide to shut down the phone is extremely limited.

Myth #5: To avoid paying telephone directory charges associated with 411 info, dial (800) FREE-411.

Truth: Some companies like (800) FREE-411 do provide free directory assistance to cell phone customers. However, users should know that while the *service* is free, your cell phone service provide may still charge you for *placing* the call.

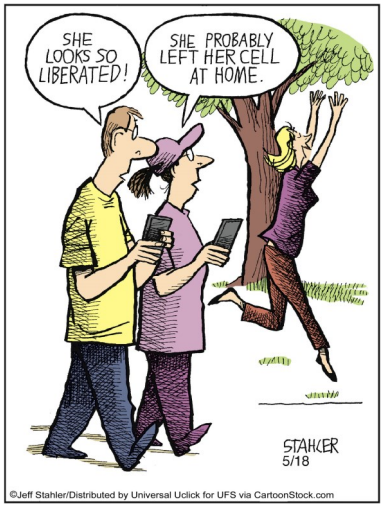
"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Justin Shelley, Master Computing

June 2015

DENTON, TEXAS

Inside This Issue…



Master-Computing.com
connect@master-computing.com
940-220-7817

MASTER COMPUTING

If Disaster Strikes, How Fast Could Your Company Be Back Up And 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 your data after a simple lightening 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!

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?

This is NOT a complete list, but it is a good start to get you thinking in the right direction.

Our FREE Disaster Recovery Plan Helps You Prepare

Since it's the New Year, we've decided to help our clients get their "IT house" in order by giving away a FREE Backup and
Disaster Recovery Audit. At no charge or obligation, we'll come to your office, review your current plan (or lack of one!) and provide a simple action plan on what you need to do to make sure your business can always be up and running.

But take note! We can only make this available to our clients and friends during the month of January; after that, the fee for this consultation will be $395. For more information, please contact our office at 940-220-7817 and ask for Justin, or e-mail us at connect@master-computing.com

3 "Gotchas" Most IT Pros Won't Tell You When Selling You Their Cloud Solution

Are you using any cloud applications to store data? Then listen up! There are a few "gotchas" you need to know about 3rd-party cloud apps that most sales reps will NEVER tell you.

1. **They aren't responsible for keeping a backup of your data.** If you read the small print of your contract, you'll see that in every way possible, your cloud provider is NOT responsible for data loss or backups – even if it's their fault. In fact, Office 365 will only keep 3 days' backup of your data; so if you delete or overwrite a file and don't notice it until 4-5 days later, it's GONE. If your data is important, you need to implement a backup solution that works with cloud applications.
2. **What you see may NOT be what you get.** There's nothing more frustrating than an incredibly slow application when you're trying to work; and the salesperson demo'ing the application or platform is going to make sure you only see the BEST-case scenarios for performance. But there are a lot of things that can determine how fast your cloud applications run, such as the file size you're working on, CPUs and RAM and storage, time of day, day of the week, your Internet connection and the number of users accessing the application. Make sure you get some verification of the speed in YOUR specific environment before spending a lot of money, time and aggravation moving to a new cloud application.
3. **What if they cancel you?** Here's a scary situation: what if your cloud provider decides to shut down your account because they go out of business or simply decide not to service you anymore? Or what if YOU want out? Make sure you have in writing what happens if YOU cancel your contract AND what your cloud provider can and cannot do if they go out of business, cancel your account or have any other issues that would cause service interruption. Moving a network from a cloud platform is NOT a simple task and you need to make sure you can get your data and that you'll be given sufficient time to make the transition.

Need help interpreting any of these scenarios? Give us a call at 940-220-7817 and we'll help you put in place a solid "Plan B" for any of the above issues.

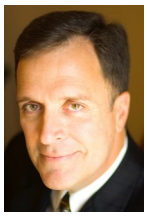
Four Ways To Get More Performance, Productivity And Profit From Your Team

1. Your Team Needs To Learn Together
Rarely do teams learn together. Too often, increases in skill are confined to individuals. Sometimes that can become a barrier to teamwork: because there are dramatically different knowledge and skill levels, some team members aren't able to keep up. When an individual attends a course or discovers a useful practice, he or she should be encouraged to share it with the team. And periodically putting the entire team into a learning environment is critical.

2. Peer Recognition Is Powerful
If you're a team leader, understand that despite your best efforts, you will be incapable of adequately recognizing every team member's efforts and contributions. Good work will slip by and go unrecognized. If this happens often, the team member may well become disillusioned. Relieve yourself of the burden to be the sole dispenser of recognition: ask team members to recognize each other. Make it a team expectation to thank other team members for their assistance and to look for opportunities to catch each other doing something praiseworthy.

3. To Win More Together, Think Together More
Have you ever held a team retreat? When was the last time your team came together for the express purpose of thinking about the work you do? Do you periodically pause as a group to reflect on what you've learned and internalize the lessons? Do you meet to consider opportunities, and not just to solve problems? The team that thinks more wins more.

4. You've Got To Expect It And Not Tolerate It If You Don't Get It
Some managers, knowing how difficult it can be to create great teamwork, undermine their efforts by making teamwork "optional." That is, they appreciate the people who are good team players but they tolerate those who aren't. As the old adage goes, what you allow, you condone. Those on the same team should know that figuring out how to get along and work with other teammates is their responsibility. Those who refuse to be team players should at the very least not enjoy the same benefits, and at worst, should be removed. It might sound harsh, but it is necessary if you want teamwork to work.



Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller *The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary,* which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

Shiny New Gadget Of The Month:

Infinite USB

As laptops grow thinner, USB ports become scarcer. This means that if you need to connect to many printers, phones, or a mouse, you need to carry around a multiport hub to plug in various devices. But Jiange has created a USB plug that is based on a daisy chain, allowing you to plug multiple devices into one USB port. It recently launched its product via a very successful Kickstarter campaign.

The design won an IF Concept Award from one of the most prestigious design competitions in the world. Jiange has a lot more design inventions underway. InfiniteUSB cables start at $10, and will also come in varieties that support microUSB and Lightning connectors.

http://getinfiniteusb.com/

WiFi Networking: What It Is, How It Works, And What You Need To Know

WiFi, or wireless networking, is quickly becoming the preferred method for connecting to the Internet or other computers because of its simplicity. Using WiFi, you can connect anywhere in your home, office, or even your local cafe without the need for wires or Internet connections.

How It Works

A simple way to understand wireless networking is to think about how walkie-talkies work. These small radios communicate by transmitting and receiving radio signals. When you talk into a Walkie-Talkie, your voice is picked up by a microphone, encoded onto a radio frequency and transmitted with the antenna to the other walkie-talkie which then converts that radio frequency back to your voice.

Where To Connect

Finding a wireless (Wi-Fi) hookup (also called a hotspot) for your laptop is getting easier. Thousands of free Wi-Fi hotspots are springing up across the country including coffee shops, hotels, and public areas.

Most of these establishments charge a fee for the access but with a little research, you won't have to pay a cent. For example, Shlotzsky's sandwich shops and Apple retail stores provide access for free to attract customers.a

Hotel chains like Best Western, Clarion, Comfort Inn and Omni hotels are also offering free Wi-Fi service to their guests. To find free hotspots in your area or an area you will be traveling to, go to ConnectedHotel (http://www.connectedhotel.com) or Wi-Fi FreeSpot (http://www.wififreespot.com). Wififreespot.com also lists libraries and public parks that offer free access. They are little bit harder to find but you may be delightfully surprised to find one in your area.

If you can't find free service, you can pay for the access. T-Mobile (http://www.t-mobile.com/hotspot/) has nearly 4,600 locations throughout the United States and has hotspots located in Starbucks coffeehouses, Borders Books & Music stores, airports and other areas.

Security Problems With Wi-Fi Hotspots

Internet users beware! Wi-Fi access is not as secure as your Internet connection at home or at work. Most free public wireless networks turn off all security functions by default to make it easier to connect.

Never, ever send a credit card number or personal information of any sort over a wireless Internet connection. The guy in the next car could grab it as easy as your neighbor. And if you set up a wireless network, remember that you must go the extra mile to ensure your network is secure. Police report a big business among criminals who use insecure networks to steal data like credit card numbers.

To safeguard your computer, turn off all file sharing and avoid sending sensitive e-mail or making online purchases.

Want To Go Wireless? We Can Help!

If you want to join the thousands of other computer users who have gone wireless, give us a call. We can install and configure the necessary hardware and software to get you connected in no time flat!

940-220-7817

How To Make Yourself 'Invisible' To Hackers

There's an old joke about two men hiking in the woods when they come across a big, grumpy black bear. Scared silly, one of the guys starts to run but notices his buddy stopped, bent-over, changing his shoes. He shouts to him, "Dude! What are you doing?!?! Why aren't you running?" to which his friend replies, "I'm changing my shoes because I don't need to outrun the bear – I only need to outrun YOU."

This is a perfect analogy for what's going on in small businesses: the "slow," easy targets are getting nailed by fast-growing cybercrime rings that are getting more sophisticated and aggressive in attacking small businesses. Last year, the average cyber-attack cost a small business $20,752, a substantial increase from 2013, when the average was $8,699. That's because most small businesses don't have the security protocols in place or the manpower and budget to implement sophisticated security systems. While there's absolutely no way to completely protect yourself other than disconnecting entirely from the Internet, there are several things you can do to avoid being easy pickings. Here's how:

1. **Lock your network.** While WIRED networks make you invisible to WiFi snoops because you have to access them by plugging into physical outlets or hacking modem ports, you can create a hidden or cloaked network on a wireless network. Simply disable the service set identifier (SSID) broadcasting function on the wireless router, and only users with the exact network name will have access. Small businesses like coffeehouses can also do this—just periodically change the network's information and place a small sign near the register with the current network name and passcode.
2. **Encrypt your data.** On your desktops, turn on the full-disk encryption tools that come standard on most operating systems: BitLocker on Windows-based PCs and FileVault on Macs. There is no noticeable performance lag; however, the encryption only applies when users are logged out of the system. So setting computers to automatically log out after 15 minutes without use is a good idea. And for mobile devices, use a VPN (virtual private network) to encrypt data traveling to and from your mobile devices and limit your employees' access to only the company data that they must have to do their jobs.
3. **Install firewall and anti-malware applications** on all of your equipment, including mobile devices.
4. **Disable features that automatically connect your mobile devices to any available network.**
5. **Disable printer and file-sharing options on mobile devices before connecting to a hotspot.**
6. **Check before connecting to hotspots.** If there is an unusual variation in the logo or name on the login page, beware…this could mean it's a fake hotspot designed to steal your data.

Can you guarantee that the person across the hotel lobby isn't looking at your data? Not really, but the chances of them being able to do that are greatly reduced if you take precautions to protect your business.

The Ultimate Small Business Guide To Setting Up A Work-From-Home System For Your Staff

You will learn:

- What telecommuting is and why so many small businesses are rapidly implementing work-from-home programs.
- The single most important thing you MUST have in place before starting any work-from-home or remote office initiative.
- How one company slashed its turnover rate from 33% to nearly 0%—and increased productivity by 18%—by implementing a work-from-home program.
- How to get a FREE "Home Office Action Pack" (a $97 value).

Claim Your FREE Copy Today at
www.Master-Computin.com/WorkFromHome

What The Heck Is A Web Site Certificate And Why Should You Care?

If you ever make purchases online, you must know how to quickly determine if the web site you are about to buy from is secure.

A secure connection is an encrypted exchange of information between the web site you are visiting and the browser you are using. Encryption of data is simply a process of converting the information you type in (your name, address, and credit card number) into an unreadable format that only the receiving web site can decipher.

Encryption is done through a document the web site provides called a web site certificate. When you send information to the web site, it is encrypted at your computer and decrypted at the web site to prevent hackers from intervening and stealing your credit card information. So how do you know if a site has a certificate and a secure connection? There are two things to look for. Just note that these two checks only apply to the web page where you actually enter your credit card information, NOT the entire site itself.

Once you are on the actual order page, look for a tiny yellow padlock in the bottom right corner of your web browser. Depending on your browser version, the Security Status bar may be located on the top of the browser and to the right of the Address bar. The padlock should be closed (locked). Next, look at the actual URL. It should begin with “https” rather than the standard “http.” If you are on a web site and you see these two things, the site will have a certificate. You can view the certificate by double clicking the yellow padlock. Upon clicking, a certificate dialogue box will pop up that contains information about who the certificate is issued to, who it was issued by, and when it expires.

Another way you can view a site's certificate is through your browser's menu options. In Internet Explorer, go to File, Properties and then click on the Certificates button. The same dialogue box will then come up for you. In Firefox, go to Tools, Page Info and then click on the Security tab. You can then click on the View button to see that site's certificate.

If you ever get a warning that there is a problem with the web site’s certificate, it could be due to a number of problems such as the names on the certificates don’t match up with the web site or the certificate has expired. If this happens, you may want to call the company and place your order by phone rather than going through their web site. Finally, make sure you check out every company’s Privacy Policy. Even if they have a secure checkout process, they could give or sell your information to third party companies.

How To Know When An Employee Is About To Quit

There's nothing quite as devastating as losing a key employee, especially if they give you no warning or notice. Often they'll give you subtle signs such as a lackadaisical approach to work, arriving and leaving on time, not a minute sooner or later, long lunches or suddenly having several appointments at the beginning or the end of the workday. But one of the biggest giveaways is their Internet behavior at work.

We already know that employees spend personal time at work on Facebook and other social media sites; but you know something's going on if they've added monster.com, Craigslist, LinkedIn and other local job sites to the web pages they frequently visit.

That's ONE of the reasons we recommend our clients install an Internet monitoring software for their network. Not only will it reveal when employees are looking for work somewhere else, it will also alert you to employees who are wasting HOURS on social media, gambling, shopping and other non-work-related web sites. It will also prevent employees from accessing porn and file-sharing sites that could bring on a BIG lawsuit or nasty hacker attack.

While some people fear this is too invasive, keep in mind that you are paying those employees to perform a job with company-owned devices and company-paid Internet. We're not suggesting you monitor their personal devices or what they do after hours on their own time. But it's perfectly reasonable to expect an employee to put in a full 8 hours if you're paying them for their time.

Of course, you should provide notice that their computers are being monitored and set the expectation that you want them working during company hours; you should also detail what employees can and cannot do with company-owned devices in your Acceptable Use Policy (AUP). If you want to give them the ability to check personal e-mail and social media sites during work hours, you can limit it to 30 minutes a day during their lunch hour or break. Again, we don't recommend this since this can be an easy gateway for viruses and hackers—but these options are available.

Need help designing an employee monitoring system on your network? Give us a call. We can help you put together an Acceptable Use Policy and put the right software in place to enforce your policy.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Greg Coleman! He was the first person to correctly answer my quiz question from last month: **What is a petaflop? a) your dog after a long walk b) the latest toy for kids c) a measure of a computer's processing speed expressed as: a quadrillion (thousand trillion) floating point operations per second (FLOPS)**

The correct answer was **c).** Now, here's this month's trivia question. The winner will receive a gift card to Fudruckers!!

June was named after the Roman goddess Juno. She was the goddess of what? a) marriage and childbirth b) fruit and trees c) religion d) love and beauty

E-mail Us Right Now With Your Answer!

Trivia@Master-Computing.com

The Lighter Side:

Lost In Translation: Advertising Blunder

- Clairol introduced a new curling iron they called the "Mist Stick" to the German market, only to find out that "mist" is slang for manure in German. Not too many people had use for the "manure stick."
- When Gerber started selling baby food in Africa, they used the same packaging as in the US that featured the "Gerber baby" on the front. Later they learned that in Africa, companies put pictures of what's inside the package on the label since most people can't read, thereby causing African consumers to think there was pureed baby inside.
- Colgate introduced a toothpaste in France called "Cue," the name of a notorious porno magazine.
- Pepsi's "Come alive with the Pepsi Generation" translated into "Pepsi brings your ancestors back from the grave," in Chinese.
- The Coca-Cola name in China was first read as "Ke-kou-ke-la," meaning "Bite the wax tadpole" or "female horse stuffed with wax," depending on the dialect. Coke then researched 40,000 characters to find the phonetic equivalent "ko-kou-ko-le," translating into "happiness in the mouth."