

**DTS**

DanTech Services

Computers under control!

Technology Times

June 2015 Issue

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 back-up 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 **907-885-0500** and we’ll help you put in place a solid “**Plan B**” for any of the above issues.



Dan Foote
Owner/President

“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!”

What’s Inside:

page 2

How To Make Yourself ‘Invisible’ To Hackers

The Lighter Side:
Lost In Translation:
Advertising Blunders

If you are ready for new phone system—watch this video!

page 3

Shiny New Gadget Of The Month:
InfiniteUSB

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

page 4

How To Know When An Employee
Is About To Quit

DanTech Clients Testimonials

The Lighter Side: Lost In Translation: Advertising Blunders



- Clairrol 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.”

Want to upgrade your obsolete PBX phone system? —click on image below and watch this video first:



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.

Shiny New Gadget Of The Month:



InfiniteUSB

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.



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

Tips from DanTech Services —TMI

We know that TMI stands for “Too Much Information” and it’s usually subscribed to getting an influx of information from someone or something that we don’t really want to take the time to know or understand or listen to. TMI is also what’s on your computer. Digging into the substrates of your computer, be it a Windows, Linux or Mac, will uncover files full of information, logs, data, and TMI. Knowing what you’re looking at or looking for when troubleshooting an issue is paramount to making that search a successful venture. Or, conversely, can turn your life into a stress-filled, anxiety ridden, tortuous path.

Frustrating for the IT tech is that Windows tends to hide things in plain view and various locations that are often missed by the normal users. A few settings changes solves these challenges revealing extensions, hidden files, and that very valuable information that may be crucial when troubleshooting problems.

Mac & Linux users have a much more open architecture when it comes to looking for parts, pieces, and data needed for problem solving. With that openness comes the responsibility of knowing what to look for, where, and why. The why might be as simple as understanding the naming conventions used or what a specific type of file or data means.

Malware, programs that can run on a computer (and all computers can be susceptible to properly crafted code), requires that “looking under the hood” that sees what’s happening within a process, script or program. Scripts or programs may cause issues as benign as monitoring web browsing activity to send you a particular result or they can be a malicious programs. Malicious programs, such as a key logger, can capture your passwords and other data, and deliver it to remote servers for the purpose of stealing your identity or accessing your bank accounts.

It’s all about the money. Consider that an exploit yields \$5 to the criminal from your account. Only \$5. Consider that across the reach of the Internet and maybe a penetration rate of .001%. Now consider the number of Facebook accounts throughout the world. We’re now talking about an incredible sum of money.

Know what you’re looking for and why. And having the knowledge to understand what you’re looking at and what it means, can save you time, frustration, and money. If there’s a suspicion that something’s not correct with a computer provides the user with choices: dig into the unknown, the substrate, and the recesses or get help. It’s our recommendation that knowledgeable help be sought. That’s what we’re here for. In some cases it’s to protect you from yourself.

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 at 907-885-0500.** We can help you put together an **Acceptable Use Policy** and put the right software in place to enforce your policy.

Recently, DanTech Services helped several clients in very different situations. One of these was too scary even for experienced and cautious Safety Manager. To find out more please click on image below and watch our testimonials:



Sam Cunard, Health & Safety Specialist, shares his experience working with DTS in emergency situation