Triangle Tech Times

MANAGED IT Solutions

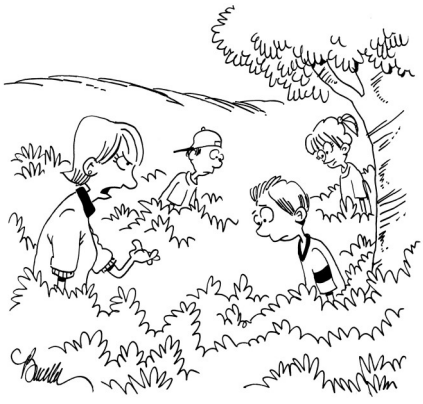
"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

♦ ISSUE 2
♦ FEB
♦ 2015

"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!"

—Rob Downs, Managed IT Solutions

A Peek Inside!



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

Broken Hearts and Stolen Data

While many people buy their significant other a box of decadent chocolates, a dozen red roses or an oversize teddy bear for Valentine's Day, there are a few people who are going to go home with a broken heart as their personal information is stolen right from under them. It's a harsh reality, but both individuals and businesses are constantly targeted by fraudsters and hackers who want to steal any bit of data that will make them money.

You may have taken all the precautions to protect yourself and your business – but what do you do if it does happen? Just as when a lover breaks your heart, you have to move on, get back on your feet and work your way through this unfortunate circumstance.

Once your data is stolen, it's gone. Credit cards can be canceled, but other information, such as your name, address, social security number and more, can be more difficult to control.

In 2014, social media accounts, such as Twitter, became more valuable to hackers than credit cards. These types of accounts are hot commodities on black markets.

Does that mean you should be worried with all the information you have stored online? Absolutely not!

If you do fall victim to a data breach, you can still protect yourself!

Contact your credit card companies. Let them know you suspect your credit card info has been compromised. They will work with you to ensure you don't face financial losses.

Keep a close eye on all your accounts. Watch for suspicious activity and report it when you see it.

Change your passwords. This is particularly critical if you used a single password for multiple services.

Use a credit-monitoring service. They aren't designed to prevent data from being stolen, but in the event of a breach, you'll be notified immediately so you can take action.

Give us a call at 919-848-3259 and we'll put together a plan to keep your company's data secure.

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
Www.palladiumnetworks.com/ITbuyersguide

How To Keep Your Laptop Secure When Using Public WiFi Hotspots

They are everywhere these days. WiFi hotspots for checking e-mail and hopping on the Internet can be found in airports, coffee shops and even most fast-food joints. But have you ever wondered, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all-time high, you are smart to be concerned. Unfortunately, it is easy for a hacker to set up a WiFi spot to access your laptop, called an "evil twin." An evil twin is a wireless hotspot that is used to lure people from a nearby, legitimate hotspot. For example, when logging in at your favorite coffee shop, you may have inadvertently logged in to an evil twin Internet connection set up by the person working on a laptop at the next table.

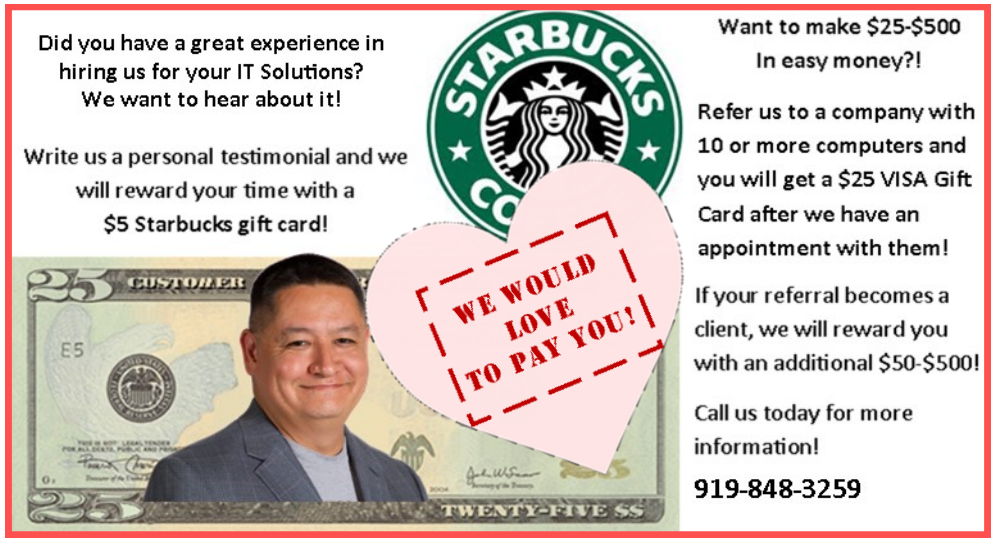
Just like legitimate sites, evil twins allow you access to the Internet, but in the background they record everything you are typing. Log on to your e-mail, investment web site or bank account, or buy something online, and they are recording your keystrokes.

Tip: Do you want an easy way to securely access your network and the Internet from anywhere? Call us today at <your phone # here> about setting up a VPN for your office!

You may be asking, "How do I protect myself at WiFi hotspots?" First you need to make sure the hotspot is legitimate. You can do this by asking someone who works at the WiFi location; in fact, some businesses will give you printed instructions that include the hotspot name. Even here you need to be careful. Many times, in an attempt to make you feel comfortable, the hacker will use an evil twin name that mimics the legitimate hotspot and, on some occasions, the fake site may even show up at the top of your network list by having a stronger signal than the legitimate site.

The best protection you can have is connecting via your company's VPN (virtual private network).

A VPN protects your online information by encrypting your data and activity even if you're connected through an evil twin. If you don't have a VPN, the best protection is to surf the net, but never type in password, credit card, social security, bank account or other sensitive information when connected to a public WiFi hotspot.



MITS Featured Client Of The Month

Carolina Case Management and Rehabilitation Services, Inc.

From its humble beginnings with three employees, Carolina Case Management and Rehabilitation Services now employs over 90 staff members. The company offers case management and expedited case resolution for medical, vocational, telephonic and specialized management services.

CCM can assist an injured employee with a worker's comp medical claim, determine his or her ability to return to work through vocational assessment and testing, perform a short-term medical case management, or coordinate long and short term disability, Director John Wells recalls the early days in 1995, when his employees recorded new client information armed with only pen and notebook.

"Electronic templates and business forms were nearly nonexistent," he laments. Having worked at IBM and Memorex Telex, John's biggest challenge was to create a strong office network and set up good, electronic ties among office and field personnel, as well as clients.

John feels an immense sense of pride in CCM's growth. "Jobs in this company are helping out 90-100 families by providing salaries to support their needs and their wants. That brings a pretty good feeling to it."

2015 marks a huge milestone in CCM's annals as the company turns 25. "We're hoping to go all out this year," he grins. "Normally, we have an all-hands, company and employee meeting each year in venues like Emerald Isle, or the Grove Park Inn in Asheville. Our 25th anniversary requires something special."

John reveals it's not just all work and no play for their clients, as well. "We like to get to know our customers, so occasionally, we'll invite them to after-hours activities like a Durham Bulls game."

As for John, his family is his priority. He enjoys travelling with his wife Nancy, who's also CCM's President and a Certified Disability Management Specialist (CDMS). An avid runner, John stays close to his kids who are all grown and thankfully, reside in the area.

Security Briefing — *Social Media Scare! Are You Being Taken Advantage Of?*

Do you use social media for your personal or business needs? Facebook, Twitter, LinkedIn, Instagram? Do you state your mind on social media? Are you open about when your birthday is? How about the birthday of your children? Your maiden name? Your mothers maiden name? Don't these all sound like typical answers to security questions? Have you ever used this type of information in a security questions? If so, you may be giving away your most valuable information on social media and practically inviting cyber criminals to steal your identity. Take a look at these 7 ways to keep yourself and your family safe while still being able to use the benefits of social media.

1. The privacy and security setting should be taken seriously.
These settings exist to help you control who sees your posts and who can contribute to your own page. Learn how to use these settings and only set them to the highest degree of which you feel comfortable. Seriously consider the differences between "public" and "friends." Be aware that the provider can (and often does) change the available settings and options at any time. Frequently review your settings and adjust for alterations.

2. Assume everything you post can never be taken back or deleted.
Even though you may be able to delete a post, this does not mean someone else has not already copied it, put it on their page or downloaded it to their computer. Think twice before posting comments or pictures. Ask yourself, "Is this something I am willing for the world to see (even potential employers or bosses)?"

3. Figure out where you draw the line on your personal information.
Do not post your birth date on any social media page. With a known year and known place of birth, it's not hard to figure out the first digits of a social security number. Other information that you post may also be used elsewhere for security verification, such as on a credit card account.

4. Only accept friend requests from people you personally know.
If you get a random friend request from someone you don't know, this someone may want to post something on your page, which, when clicked, will direct your friends to a site that will downloads a virus. Sometimes the difference is someone looking at the post and saying to themselves, "oh, this is a friend of Susan's" and thinks that it's an implied endorsement.

5. Be informed on what to do if someone is harassing or threatening you or your family via social media.
If you do become a victim, do not be afraid to take steps to protect yourself. Take a picture of the threat, remove that person from your friend list, block them and report to the site administrator and law enforcement, if applicable. Take threats of physical action and violence seriously. A threat is a threat.

6. Be careful about installing extras on your site.
Some social media sites allow downloads of third-party applications for games and other things. These applications could be malicious in nature. Take the same safety precautions that you take with any other program or file you download from the web. Review the access permissions. Just as with mobile application permissions, you can frequently identify potential problems in advance by recognizing excessive permissions. (Why does the app need to post on my behalf, know my location or see my contact list?)

7. Talk with your kids about social networking.
If you are a parent of children who use social networking sites, Microsoft has some solid advice for kids on how to use social websites more safely. View the information at www.microsoft.com/security/family-safety/kids-social.aspx .

Taken from source "www.soluitonary.com"

Did You Know That Managed IT Solutions Offers...

File Sync and Backup

Did you know that Managed IT Solutions offers a file Sync and Backup solution. This is used primarily when you have the need for a simple way to share your files with colleagues or across your other devices. It also allows you to backup your files and folders. Palladium SYNC will give you secure access to data on all types of devices and can allow for safe

uncompromised partnering of your data with others. Our SYNC solution offers secure anytime access, no matter where you are, to all your file server data. This solution works with devices such as PCs, Tablets and Smart Phones. If you have a need for a quick and easy file sharing and backup solution, give us a call today to start new services.

Get THREE For FREE!

Sign up today with Palladium SYNC and receive your first THREE months for FREE. This offer is only available until the end of March so call us at (919) 848-3259 to receive your 3 free months of Palladium SYNC File Sharing and Backup Solution.

- Backup Files and Folders
- Share Data Safely Across Devices
- Share Data Safely With Associates
- Get Secure Access To Your Files Anytime, Anywhere
- Includes 20GB Of Storage Per Account

If extra storage is needed we offer packages with larger amounts available. Please call us for details.

After your first 3 free months of service you may choose to continue our Palladium SYNC solution for just $10 a month per account.
Keep your files backed up and secure.
Call Us Today At (919) 848-3259

HOW TO GROW STAR PERFORMERS

A study of computer programmers at Bell Laboratories showed that the star performers outperformed moderate performers by a margin of 8 to 1. If that holds true in your organization, the conversion of five of your moderate performers into star performers would be the equivalent of adding 35 moderate performers to your workforce. Where are you going to find the five additional star performers? You don't find them. You develop them.

The Bell Labs study identified nine work strategies that characterize star performers. All of them are qualities that can be inculcated through a good corporate education system. According to researchers Robert Kelly and Janet Caplan, these qualities are:

1) **Taking initiative:** accepting responsibility above and beyond your stated job, volunteering for additional activities and promoting new ideas.
2) **Networking:** getting direct and immediate access to coworkers with technical expertise and sharing your own knowledge with those who need it.
3) **Self-management:** regulating your own work commitments, time, performance level and career growth.
4) **Teamwork effectiveness:** assuming joint responsibility for work activities, coordinating efforts and accomplishing shared goals with workers.
5) **Leadership:** formulating, stating and building consensus on common goals and working to accomplish them.
6) **Followership:** helping the leader to accomplish the organization's goals and thinking for yourself rather than relying solely on managerial direction.
7) **Perspective:** seeing your job in its larger context and taking on other viewpoints, like those of the customer, manager and work team.
8) **Show-and-tell:** presenting your ideas persuasively in written or oral form.
9) **Organizational savvy:** navigating the competing interests in an organization, be they individual or group, to promote cooperation, address conflicts and get things done.

Star performers considered initiative, technical competence and other cognitive abilities to be core competencies. Show-and-tell and organizational savvy were on the outer edge of their circle of importance. Middle performers placed show-and-tell and organizational savvy at the center. While star performers were focused on performance, middle performers were focused on impressing management.

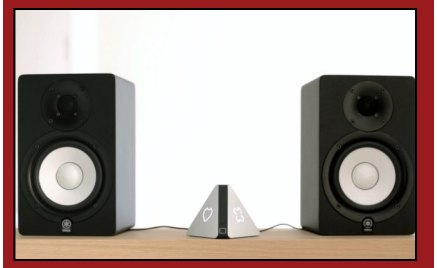
Star performers and middle performers also showed marked differences in their attitudes toward networking. The middle performers waited until after they had encountered problems before looking around for someone who could provide help and support. The star performers built a network of helpers and supporters in advance, so they could call on them immediately when needed.

The study concluded that "Individual productivity… depends on the ability to channel one's expertise, creativity and insight into working with other professionals."

Star performers emerge from educational systems tailored to the individual company and the individual job. They don't want to become clones. Too many companies today are content with training programs that provide people with knowledge and expertise, but skimp on educational processes that teach them to apply what they learn. You can't train them to seek excellence. You change that attitude through consistent input that appeals to an individual's self-interest and organizational spirit.

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

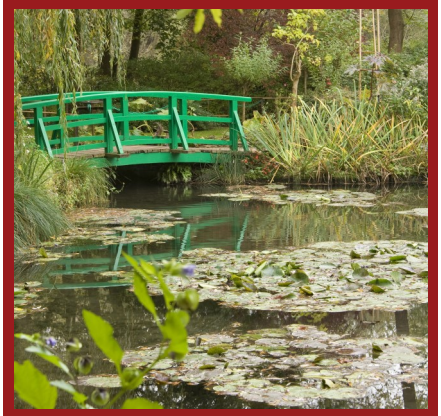
This month's gadget is so new, it isn't even off the assembly line. Meet Prizm — a small, pyramid-shaped device designed to make your home-audio experience as hands-off as humanly possible. The device was recently backed on Kickstarter this past November. The French company behind the audio device wanted 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.

The Lighter Side:

Punch a Painting, Go to Prison



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.

Protect Yourself From Online Credit Card Fraud

The past couple of years have been a rough ride for anyone who relies on a credit card to make purchases. Data breaches have plagued retail stores in the U.S. and Canada. Credit card providers are set to roll out new, more secure credit cards to consumers this year, catching up to Europe and much of Asia in terms of credit card security. The U.S., in particular, has lagged behind in credit card security due in part to the cost of upgrading both the cards themselves and the pay terminals.

If you are concerned about your credit card information falling into the wrong hands, there are several steps you can take to protect yourself:

- **Only give your credit card information to secure and trusted web sites.** Never enter any personal or financial information on a non-secure web page. If you don't see "https" in the web address, move along.
- **Monitor all activity.** Regularly check your credit card and bank statements. The simplest way to spot fraud is to monitor all your financial activity. Many credit card providers have custom alerts you can set to notify you if certain purchases are made.
- **Never save credit card information.** Many online retailers and shops now ask if you would like to save your credit card information for future use. While it may seem convenient, skip it.
- **Delete your cookies and auto-fill data.** When you enter information on a web page, that data is stored in your web browser. After you complete a transaction, go into your browser's options, settings or history tab and delete the data.