Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
February 2020

Want to Relieve Some Stress?

Have you ever been so mad at your computer that you just wanted to smash it to pieces?

Good news, now you can! Well, sort of...

Just submit to us your most embarrassing, frustrating, or funniest technology moment for your chance to smash a computer! Take out all your frustrations on one of our previously DOD wiped computers with a sledgehammer and we'll bring coffee and cake for the entire office.

We'll provide the computer, the sledgehammer, and the cake and coffee, you provide the story and the angst.

It's a win-win.

Simply email us your technology story to Marketing@CTTSonline.com

Winners will be chosen and notified on Monday, February 24th.

This monthly publication provided courtesy of CTTS, Inc.

If You Think Your Business Is Too Small To Be Hacked... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die. And that's not an understatement!

Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

> **"The reality is that cyber security should be a normal, everyday part of any business."**

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats, and many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen" or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet and if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability!

You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company.

There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

Free Report Download:
The Business Owner's Guide To IT Support Services And Fees

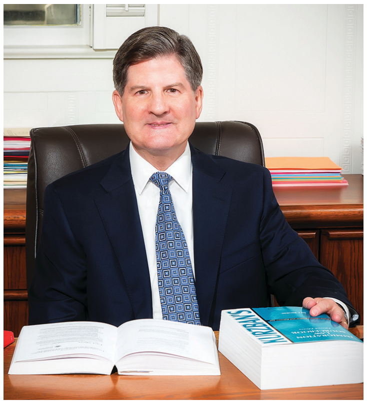
You'll learn:

- The three most common ways IT 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.

Simply visit www.CTTSonline.com/ITBuyersGuide or call (512) 388-5559 to claim your free copy today!

PP Paul Parsons PC
ATTORNEY AT LAW

Client Spotlight: Immigration Law Office of Paul Parsons P.C.



Since 1978, Paul Parsons has been providing legal immigration representation for companies of all sizes and for individuals from around the world, including from Mexico, Canada, China, India, Iran, and the UK.

Locally based in a small office on Rio Grande Street, the Immigration Law Office of Paul Parsons P.C. has been helping immigrants in downtown Austin for the past 40 years. His firm specializes on representing U.S. citizens seeking permanent resident status for their spouses, parents, and children, and seeking U.S. citizenship (naturalization) for people who already hold green cards. While their office is small, they're doing big things.

One of Mr. Parsons' favorite success stories comes from a woman from Central America named Abby. She entered the U.S. with a 30 day visitor visa and fell in love with the culture, people, and everything else about our wonderful country we are so lucky to inhabit.

Over 20 years passed and she constantly worried about not having proper immigration documents. Finally, she fell in love and married a U.S. citizen. Mr. Parsons was able to represent Abby to obtain U.S. permanent residency status despite having overstayed her visit. At last she was able to return to Guatemala to see her mother, sisters, and even meet for the first time nieces and nephews. Later, Mr. Parsons helped Abby qualify for U.S. citizenship.

What appears to be paperwork are actually confusing applications, petitions, and supporting documentation needed by persons who are eligible for green cards and citizenship. Some cases take years due to government backlogs and visa waiting lists. An employer-sponsored green card case usually involves one state and three federal agencies (U.S. Citizenship & Immigration Services, Department of Labor, and Department of State).

The multiple complications that can arise and delays involved are stressful not only for the clients, but also for the lawyers. "Being an immigration lawyer is very stressful but brings tremendous satisfaction when a client's case is approved," Mr. Parsons said.

Although the obstacles one faces in the multi-step process to become an citizen are great and varied, Abby never gave up hope and Mr. Parsons will never forget when she said, "Mi esperanza nunca murió," which translates to, "my hope never died." It can be easy to lose sight of hope when your livelihood is under serious scrutiny and numerous difficulties arise, but that's why Mr. Parsons and his team are so dedicated to their clients and their individual situations.

Each case in Mr. Parsons' office is not just a number, but a person's story. This humanization of the bureaucratic process is one of the many things that sets them apart from many other immigration law offices and makes them the leading immigration law office in the Austin community.

> **"Mi esperanza nunca murió," which translates to, "my hope never died."**

Mr. Parsons' integrity and understanding of the multiple aspects of the Latin culture helps to build his clients' trust which is critical for success.

When he was just 17 years old, Mr. Parsons participated in an international student exchange program at his high

Client Spotlight: Immigration Law Office of Paul Parsons P.C.

school. Growing up in Oklahoma, he had never ventured outside of the country until staying with a family in Quito, Ecuador. The family took him in as one of their own. During his exchange program, he developed a love for Spanish and the Latin American culture and people.

TRAVEL DOCUMENT
U.S. DEPARTMENT OF HOMELAND SECURITY
Issued by U.S. Citizenship and Immigration Services
PERMANENT
Category IR1

When Mr. Parsons started law school, he wasn't exactly sure how, but he knew he wanted to incorporate Spanish into his career. In his 3rd year at the University of Texas School of Law, he attended the law school's very first immigration conference and it clicked. He knew he wanted his specialty to be immigration law.

The late Houston-area immigration attorney, Sam Williamson, has always been an inspiration for Mr. Parsons and his colleagues. Nationally known for his extensive 60+ year career in the immigration field where he fought fiercely for the rights of his clients. Mr. Williamson instilled in Mr. Parsons the values of being honest and truthful with clients without giving them false expectations.

Mr. Parsons' professional and efficient reputation is widely evident not only in the countless positive reviews from clients, but in the numerous awards he has received. Rated as a "Super Lawyer" for over 10 years, Mr. Parsons is also recognized by Best Lawyers, and holds a "Superb" Avvo rating.

As with all industries, technology continues to play a major role in every aspect of business, including Mr. Parsons' law offices. From the specialty immigration case management software, LawLogix, to other business applications like Outlook, Excel, and all the other apps that come with Office365, technology is at the center of it all. Between emailing different government agencies and updating clients on the status of their cases, to specialty software needed to prepare applications, petitions, and supporting documents, it would be impossible to operate their immigration firm without their computers running smoothly.

Email communication is a key aspect of their practice. Immigration is so important to individuals that frequent status updates and reassurances are vital.

As a client with CTTS since 2015, we proudly manage Mr. Parsons' business technology, including email, data backup and disaster recovery for business continuity, VoIP communications, and we've recently upgraded his email to have encryption for sensitive documents.

Support Specialist, Jamie Myers commented, "I love how security conscious Mr. Parsons and everyone at his law office are, their attention to detail only aids in our cybersecurity efforts."

Between Mr. Parsons, their Associate Attorney, Bernadette Dela Cruz, and their support staff, they have 10 desktops and a server managed by CTTS. We keep their business-critical data and email professionally managed and backed up with monitoring software and backup appliances like Datto WorkPlace, Maraki, and Backupify. This means that in the event of a disaster situation, whether it be due to human error, natural disaster, or cybercriminal related, they can restore from one of the several save points that perform this business saving service behind the scenes.

Like all our managed services clients, their critical business data is covered by Sentinel One endpoint security and Cisco Umbrella - which means they are protected from threats like ransomware and other data breaches with real-time forensics and proactive notifications.

With continued client success stories comes business growth, and with CTTS, the security of Paul Parsons Immigration Law Office will grow along with him, and we're excited to be there every step of the way.

If you'd like more information about Paul Parsons PC, Attorney at law, visit, **https://www.immigrate-usa.com/** or call their office at (512) 477-7887.

3-2-1 Backup!

Quarterback, linebackers, cornerback, running backs and back up players – who is ready for the Superbowl? Having an effective backup strategy in place is essential in any endeavor, whether it's in sports or in your business. How, where and what you back up makes a major difference in your ability to recover should disaster strike.

There is a well-documented industry best practice standard for backing up your critical data. It is known as the 3-2-1 Backup rule: Have at least t**hree copies of your data**, Store the copies on **two different media,** Keep **one backup copy offsite**.

Sounds pretty good, right? It is, but there is more to consider than just backing up your data, i.e. your files. Let's suppose you could back up all the personal items you have in your house—your clothes, furniture, valuables, etc., and somehow maintain a copy of everything in a warehouse 1,000 miles away from your current residence. Now let's suppose (and God forbid) your house burns down, destroying everything with it. You'd be relieved that you had a copy of everything somewhere else.

But here's the problem: If your house burned down, you might have a copy of everything you own, but you no longer have a place to put it. So, for starters, you have to rebuild the house. Next, you have the project of getting everything out of that storage unit into your NEW house. Then you have to rearrange everything. This is exactly how most backup systems work UNLESS you are running "image" backups. An image will allow you to restore your server, PC, device, etc., FAST because you're not backing up single items but, instead, the ENTIRE HOUSE.

Call us at **512-388-5559** to see how a solid disaster recovery strategy can help you safeguard your business in the event disaster strikes.

3 Reasons Why Recessions Are Awesome For Great Companies

It may be jarring to read the words "recession" and "awesome" in the same sentence. Recessions are bad for most people. I will not make light of how horrible recessions are for the vast majority of companies and their employees, (as well as for not-for-profit organizations and governments).

For most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, increased board and shareholder pressure, increased financial strain and a feeling of looming danger in the pit of your stomach, which is no fun to wake up to every day! But for great companies, recessions can be awesome.

What are great companies?

Great companies make great products or deliver great services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take great care of customers and employees, great companies don't have a dangerous debt burden. They are profitable and able to pay their bills to suppliers while delivering an attractive return to investors in dividends and equity appreciation.

How are recessions awesome for great companies?

Recessions allow great companies an opportunity to do the following:

1 Shake loose the cobwebs of complacency.

"Success breeds complacency," said Andy Grove, the legendary CEO of Intel. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace (Only The Paranoid Survive), I am here to suggest that great companies have to keep hustling to stay great. A recession provides an opportunity for a wake-up call to great companies that may start to coast on past greatness and help them get back on track.

2 Take customers and colleagues away from lesser companies that don't deserve them.

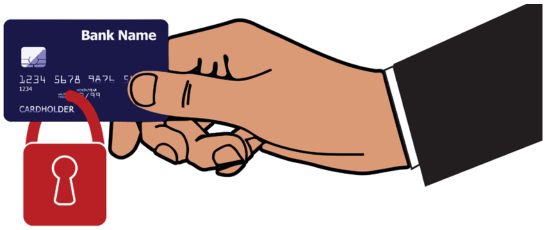
As lesser companies stumble during recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more customers and talented people. I remember when a successful business services company with 70 locations around North America entered the '08 recession. Lesser competitors were closing branches and laying off people, and service was slipping. But the CEO of the successful company was not fearful about the recession. Instead, he sensed the opportunity to win more customers with better service and poach some top talent away from the struggling competitors. The recession allowed this great company to gain market share and build a stronger leadership talent pipeline.

3 Increase the rate of learning of your leaders.

Time seems to move more quickly for me during harder times than during easy times. This can improve the learning curve of your up-and-coming leaders. Just remember to not make too many decisions for them; that will stunt their growth. Allow your leaders to come to you with problems and solutions, and coach and support them. Let them test and learn various approaches to leading through uncertain times.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, Who: A Method For Hiring, and the author of the No. 1 Wall Street Journal best seller Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

7 Things To Do So You DON'T Get Hacked When Shopping Online



1. Verify the URL is safe.
Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate.
Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser.
Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments.
Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites.
When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager.
It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores.
If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

Top 2 Tips For Scaling Security For Your Small Business

Put a greater emphasis on passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA).
MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security.

Did you miss it?

Check Out Last Month's Top Tech Tip:

Tech Tip #155: Save Time With Our Top 3 Chrome Shortcuts

Not enough time in the day?

To help you work more efficiently and improve your bottom line, I have scoured the internet to bring you the top 3 shortcuts for Chrome that will save the day...

By Kyle Barker

Read it Here: http://bit.ly/Tech-Tip-155