

CTTS TECH TALK

*For Humans
Not Geeks!*

Your resource for the latest technology updates and opportunities for your success.




Central Texas
Technology Solutions

What's In This Issue?


Your Tech Tip of the Month

What Key Change Could Your Business Benefit From?

3 Ways To Protect Your Data During COVID

Everyone On Your Team Needs Cybersecurity Training.

Please Welcome Your Newest Support Technician, Kyle Tyre!

CTTS, Inc.
 (512) 388-5559

You NEVER See It Coming! But Once It Hits, Everyone Says, "I Wish I Would Have ..."

A year ago, no one could have predicted that countless businesses would shift to a remote work model. The pandemic hit hard and fast! Small businesses had to think on their toes, and many had only a few weeks to adapt. It was stressful and extremely challenging.

Looking back on it, many SMBs wish they'd had a plan in place which would have made things easier. When the pandemic hit in February/March 2020, SMBs had to absorb the huge cost of getting their employees up and running off-site. Not only was it costly, but it also took a lot of coordination and on-the-fly planning. This meant things slipped through the cracks, including cybersecurity.

As they say, hindsight is 20/20. You may wish you had a plan in place or had more time, but you didn't. A vast majority didn't. However, you can still plan for the future! While you never know when disaster is going to strike, you CAN be prepared for it. Whether that disaster is a pandemic, flood, fire or even hardware failure, there are steps you can implement today that will put you in a better place tomorrow.

Here's how to get started.

Put Your Plan Into Writing.

First and foremost, you should have a standard operating procedure to call on should something go wrong. For example, in early 2020, many SMBs didn't have a security



plan in place, let alone a remote work security plan. They had to make it up as they went, which just added to the challenges they were already experiencing.

To get over this challenge, work with an experienced IT services company or managed services provider (MSP) to put together a plan. This plan should include a cybersecurity protocol that defines what malware software employees should be using, what number they should call for 24/7 support, who to contact when they receive suspicious e-mails, how to identify suspicious e-mails and so on.

“When you have IT security... you put your business and all your employees in a much better place.”

More than that, it should outline exactly what needs to happen when disaster strikes. Pandemic? Here's how we operate. Fire? Here's what you need to know. Hardware failure? Call this number immediately. The list goes on and can be pretty extensive. Again, this is why it's so important to work with an MSP. They've already put together plans for other SMBs. They know where to start when they customize a plan with you.

Invest In Security And Backups.

While every business should have network security already in place, the reality is many don't. There are a ton of reasons why (cost concerns, lack of time, lack of resources, etc.), but those reasons why aren't going to stop a cyber-attack. Hackers don't care that you

didn't have time to put malware protection on your PCs; they just want money and to wreak havoc.

When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place. All of this should be in place for both on-site employees and remote workers. With more people working from home going into 2021, having reliable IT security in place is more important than ever before.

On top of that, you should have secure backups in place. Investing in cloud storage is a great way to go. That way, if anything happens on-site or to your primary data storage, you have backups you can rely on to restore lost or inaccessible data. Plus, having a solid cloud storage option gives remote employees ready access to any data they might need while at home or on the go.

Where Do You Begin?

Some SMBs have the time, money and resources to invest in on-site IT personnel, but most don't. It is a big investment. This is where partnering with an experienced IT services firm can really pay off. You may have employees in-office or you may have a team working remotely – or you may have a mix of both. You need support that can take care of everyone in your organization while taking care of the data security of the business itself. This is where your IT partner comes into play. They are someone you can rely on 24/7 and someone who will be there for you during a pandemic or any other disaster.

Your Tech Tip of the Month

Troubleshoot Your Printer in 5 Steps



As we all know, printer functionality directly effects the productivity of our office. Below are 5 steps to troubleshoot your printer before throwing in the towel:

1. Check for Power - You never know!
2. Check for an Error Message
3. Check Cable and Network Connections
4. Try Printing Test Pages
5. Check Print Drivers

Hopefully you can now successfully hit the 'Print' button and have it spit out your pages by the time you make your way to the printer. If further troubleshooting is needed, call us today: **(512) 388-5559**

To read the entire article, visit: bit.ly/Tech-Tip-208

What Key Change Could Your Business Benefit From?

You could say that we're all experts at change, now. After last year, even those who were resistant to change have passed a masterclass in adaptability.

When you're running a business, change isn't a bad thing. That's also true when it comes to the technology you use.

Your IT setup should be something that's been well thought through. It should allow your business to change and adapt with minimal stress.

However, if you don't have an IT service partner working **proactively**, you might be missing that.

It's one thing having an IT support company waiting to fix things for you. It's another having a partner who's constantly looking at your setup and designing ways to make your team's lives easier both now and in the future.

This is what we do and we'd love to do it in partnership with you.

You see, we're confident that after spending a little time on a call with you, we could identify some areas for key change that could make a huge difference to your business and its IT setup.

We're calling this our Key Change Audit. Snappy, eh?

During this audit, our experts will take a detailed look at your IT infrastructure, what you do and the tools you currently use to do it. We'll discuss how you'd like everything to work in an ideal world. Then we'll make suggestions on the key changes you could make to get your setup as perfect for you as possible.

Call to schedule your free audit now: (512) 388-5559



3 Ways To Protect Your Data During Covid

1 Manage Your Passwords. You've heard it before, and you'll hear it again – one of the best ways to keep intruders out of your data is to lock it behind strong passwords that are updated every 60 to 90 days. Use passwords that are a mix of letters, numbers and special characters. Make passwords long and confusing.

2 Secure All Data. Who are you sharing your data with? Do former employees still have access? What about former clients? Take time to see who has permission to access your network and data. While you're at it, clean up old or useless data that may be just taking up space. When you know what data you're saving – and who has permission to access that data – you can better protect it.

3 Adopt Best Practices. When was the last time your team received IT security training? Never? Five years ago? It's time to get back on it. Train your team on the latest cybersecurity threats and how to handle them. Then, adopt best practices so your team knows what to do when they receive a phishing e-mail or there's a threat to your network.



Everyone On Your Team Needs Cybersecurity Training. Including You.

Every good business leader knows that training is essential for a highly productive team.

But have you ever considered giving your staff cybersecurity training? You really should.



What is it?

It's about increasing their awareness of the ways that criminals try to break into your IT system, and the devastating consequences if they do.

So, they learn:

- How to spot the different types of fake emails and messages, and what to do with them.
- The risk of social engineering by email, phone, or text message.
- Why we use basic security tools such as password

managers and multi factor authentication (where you generate a code on another device)

By holding regular cybersecurity training sessions, you can keep everyone up to date. And develop a great culture of security awareness.

It's another layer of protection to help ensure that your business doesn't become part of a scary statistic (one small business is hacked every 19 seconds).

P.S.

As the leader it's critical you do the training, too. You'll be one of the most targeted people in the business, as you probably have access to all the systems, including the bank account (s).

How can I make my WiFi faster?

Try moving your device closer to the router. If that works you may need to install some access points to extend your range. Connect directly to the router with a cable. If it's still slow, call your provider to see if they can work their magic at their end.

Why can't I print?

Try moving your device closer to the router. If that works you may need to install some access points to extend your range. Connect directly to the router with a cable. If it's still slow, call your provider.

What do I do when my computer crashes?

Annoying. First, give it a couple of minutes to see if it fixes itself. If not, open your task manager, see what program is not responding and close it. If that doesn't work, restart the device, and try again. If it happens repeatedly, call for help!

Submit Your Question Here:
Marketing@CTTSONline.com

Please Welcome Kyle Tyre!



As our newest support technician, Kyle will assist our clients with any technical issues or questions they may have to ensure their technology does not interfere with their business productivity.

An Army veteran, having served for 8 years in various places around the world, Kyle has been working in the tech industry for about 12 years now including his time in the military. Most recently, he spent time as a desktop support specialist at a financial institution prior to coming to CTTs.

Originally from North Texas, Kyle has been in Central Texas since leaving the military. He enjoys spending time with his wife and two daughters and their dog, playing video games, enjoying family board game nights, and traveling.

This is how you can get in touch with us:

call: (512) 388-5559 | email: info@CTTSONline.com
website: www.CTTSONline.com



Follow Us

