Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984

Did you know...

We can also help you save THOUSANDS on your current phone costs!

We have VoIP business phone systems that can deliver cost savings without sacrificing the call quality and dependability of a landline.

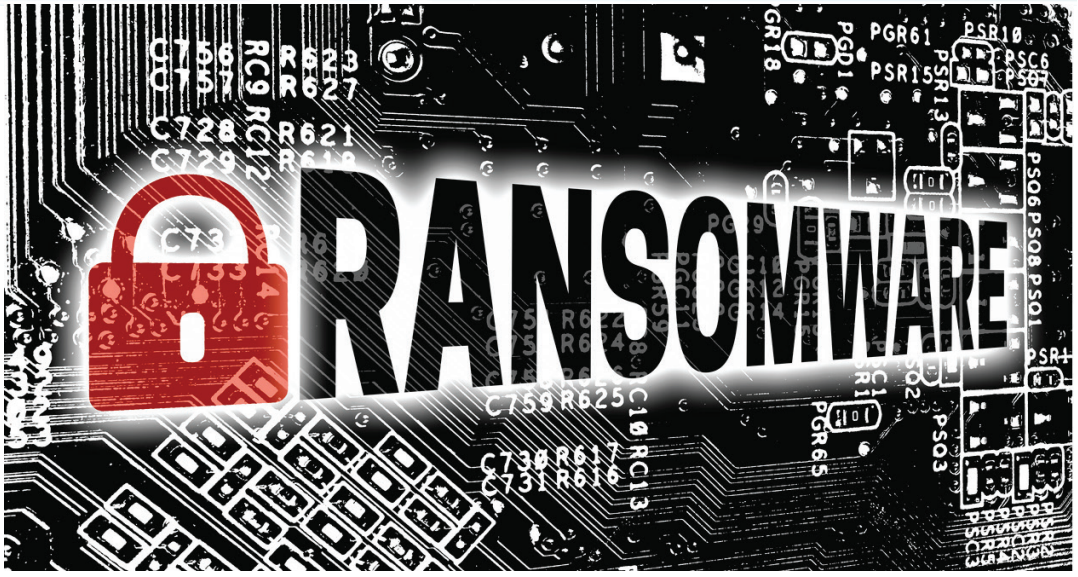
Call us today or email me at ryan@computer-service.com to talk about how we can start to save your business money. Or you can download the report I wrote about how to choose the right VoIP system at:

www.computer-service.com/betterphones

April 2018

This monthly publication provided courtesy of Ryan Haislar, Vice President of Computerease.

"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!"



City Of Atlanta Falls Victim To Ransomware: A $51,000 Ransom and 6+ Days Without Computers

At 5:40am on Thursday March 23, 2018 the city of Atlanta fell victim to a ransomware attack. A ransomware attack encrypts critical data and files on computers and networks, holding it hostage unless a ransom is paid.

As of Thursday March 29th (when I'm writing this article) the city still hasn't decided whether or not they will pay the ransom of $51,000 demanded by the hackers to regain access to their files and computers.

For 6 days the city has been crippled, the municipal courts have been closed, police officers are filing reports by hand and city employees have not been able to use their computers.

The Mayor of Atlanta, Keisha Bottoms, announced the creation of a response team to help resolve the crisis. This team has been working around the clock since and include the federal Department of Homeland Security, the FBI, the Secret Service and cybersecurity experts from Georgia Tech.

So far there is no evidence of personal data being exposed to the hackers, however authorities are advising all residents to proactively monitor their bank accounts and credit reports as a precautionary measure. They are still not sure of the full extent of data that has been compromised as the result of this cyberattack.

The City Was Warned Of Their Vulnerability To Cyberattacks, Yet Did Nothing

According to a recent NPR article, there was an audit of Atlanta's IT department that indicated that there was significant risk within their computer networks and systems that left them vulnerable to a cyberattack. NPR's Emily Cureton reported, "The audit found *<continued Page 2>*

a significant level of preventable risk to the city. The audit report details that there were long-standing issues, which city employees got used to and also didn't have the time or resources to fix." The report also continued, "The audit of the IT systems concluded that Atlanta had no formal process to manage risk to its information systems."

There are even reports from a Georgia-based cybersecurity firm, Rendition Infosec, that at least 5 computers were previously infected with a different strain of ransomware in April 2017.

"Paying a ransom doesn't guarantee an organization that it will get it's data back - we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive to get involved in this type of illegal activity." FBI Cyber Division Assistant Director James Trainor

This Could've Been Prevented

The unfortunate thing about this story is that there are numerous ways in which this attack could have been prevented. It appears that more than one firm provided warning to the City of Atlanta that they were vulnerable and yet they seem to not have heeded the advice.

And, the type of prevention needed is affordable - even to small businesses. We have a large number of very affordable cybersecurity solutions which when layered together significantly reduce the risk of these types of attacks. Even something as simple as a good offsite or 'cloud' backup solution would have allowed the city to be back up and running more quickly without having to consider paying the ransom.

Paying The Ransom Is Not A Sure Thing

Even if the city of Atlanta decides to pay the ransom, there is no guarantee that their problems would be solved. In a 2016 report about the risks on ransomware attacks, FBI Cyber Division Assistant Director James Trainor wrote, "Paying a ransom doesn't guarantee an organization that it will get it's data back – we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity."

There is no one way to respond to these ransomware attacks. The ONLY true way to protect your business is to have multiple layers of preventative cybersecurity solutions in place to keep your data and client information safe and the cyber criminals out.

"But My Business Is Too Small… There's Nothing Worth Taking…"

I hear that all the time and frankly, those are the cybercriminals ideal targets. As a business, you almost certainly have one or more bank accounts which cybercriminals would love to drain. You may also have patient or client data which is valuable on the dark web. Or, if you are like the City of Atlanta or the St. Louis Public Library System you have files which you might be willing to pay to get back. (Or you might pay and still not get them back. These are criminals after all)

Please don't let your business be the next victim, contact us and let us implement a best-in-class cyber security solution for your business. You can call me direct at (314) 432-1661 (MO) or (618) 346-8324 (IL) or email me at ryan@computer-service.com.

Cutting Edge Ransomware Protection: Sentinel One

Once I saw this software in action, I knew that I had to make this available to our clients. This a game changer in the fight against Ransomware. This NextGen Antivirus software is used and trusted by large corporations to anticipate and block NEW cyberthreats, not just previously recognized ones. It can literally "undo" encryption damage caused by ransomware!

1 in 5 small businesses will suffer a cyber breach this year.
81% of all breaches happen to small and medium businesses.
97% of breaches could have been prevented with today's technology

Check out a live demo of this powerful software on our website:
www.computer-service.com/sentinelone
Or call us today at (314) 432-1661 (MO) or (618) 346-8324 (IL)

Latest Webroot Cybersecurity Feature: DNS Filtering

I sat down with Cameron Stone from Webroot during a recent IT conference in Arizona and we discussed the new Webroot DNS filtering service which we can now offer to our clients. You can check out the video on our website at: www.computer-service.com/DNS

DNS filtering is an additional layer of security which we can add to our clients existing security solutions. Our managed clients have security enabled firewalls which a great deal of protection inside the office network. However, the new DNS filtering service from is still a good addition even for computers which remain inside the office.

However, computers which travel outside of the office do not have quite the same level of protection as they are not behind the office firewall. So, adding DNS filtering capability to individual computers provides an additional layer of protection for those devices when the leave the office.

One of the best parts of the Webroot DNS filtering services is that there is no installation required if the computer already has our standard Webroot Antivirus agent. We can simply turn the DNS Filtering feature on with the flip of a switch. Contact us today to add Webroot DNS Filtering to your cybersecurity solution.

19 Ways To Live Well And Sanely In Crazy Times

There's no discounting the fact that we're living through some crazy times. With political upheavals, game-changing social media movements and chaotic world events, there's a lot going on.

I'm not about to overlook the tremendous opportunities that exist these days, but with spring cleaning right around the corner, I've been focusing on this question: How can we live well in these crazy times?

1. Don't add to the craziness. Be civil to those with whom you disagree. Balance your heart and your head so emotions don't outweigh reason.

2. Separate fact from opinion. Don't get excited about things that either aren't true or are wildly exaggerated to get attention. Daniel Patrick Moynihan said, "Everyone is entitled to their own opinion, but not to their own facts."

3. Act with integrity even when others don't. Just because others are behaving badly doesn't mean you should too.

4. Slow down. The longer I live, the more convinced I am that you accomplish more of real importance by slowing down. Speed is necessary at times, but make sure you're not chasing rabbits when you could be tracking the big game.

5. Eat slower. A friend's father-in-law was a doctor, and when asked what was the most important thing a person could do to improve their health, he said "Chew more."

6. Get enough sleep. Lack of sufficient sleep is a major influence on poor health, both mentally and physically.

7. Read for education and entertainment. The best novels aren't just engaging, they teach us something about the world and about ourselves. In addition, read about current events and personal development to keep well-rounded.

8. Limit your news intake. Being saturated with more of the same, day in and day out, can be fatiguing and frustrating. Be informed, but not inundated.

9. Exercise. It's as simple as that.

10. Have deeper conversations with friends. Go beyond, "How's it going?" to "What are you thinking?" Move past the superficial and really connect.

11. Take a trip. The best way to enlarge your perspective is to travel abroad. But if you can't, for whatever reason, visit a new state or spend time in a museum.

12. Be civil.

13. Be kind.

14. Count your blessings every day. To be precise, list at least three. No matter how bad it gets, there are always things to be thankful for.

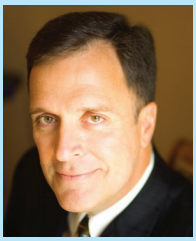
15. Spend less than you make.

16. Invest more in experiences and less in stuff.

17. Live intentionally. Be specific about what you want to accomplish each day. Don't sleepwalk through your life.

18. If you can't take action to deal with something, don't worry about it. And if you can, then do it and stop worrying!

19. Tell people you love that you love them. You'll rarely regret telling someone that you love them, especially when you no longer have the chance to do so.



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the bestselling author of books like Fred Factor *and* The Potential Principle *and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*

Cyber Liability Insurance: An Essential Protection For Your Business

Cyber liability coverage is NOT INCLUDED with typical business insurance and it is required that you add it to your existing plan. Without cyber liability insurance you will be paying for expenses related to a cyberattack OUT OF POCKET. We are advising all of our clients and other business owners to make a simple phone call to their business insurance agent and add cyber liability insurance today!

Follow These Basics To Help Protect Your Company From Cybercrime Modern businesses spend a lot of time and resources protecting themselves from the latest scams and cybercrimes, but it's important not to lose sight of the basics. The same goes for your team. Everyone in the company should be well-versed in essential security principles. Security protocols should be thoroughly documented and included in every new employee's training. Strict policies for violating these items should also be detailed.

Your security plan should mandate strong passwords, requiring users to only ever connect to the network via VPN, with guidelines for regular password changes. A little prevention goes a long way — remembering the security basics and doing some research are the best ways to protect yourself and your company.

Do These Things to Keep Your Best Employees From Leaving According to the Gallup's 2017 "State of the American Workplace" report, 51% of currently employed adults in the U.S. are on the hunt for a new job, using company time to search far and wide for a better opportunity. How can you prevent this trend from forcing your best people out of your company?

First, you should give the best people in your organization abundant opportunities to move around and apply their strengths where they're best suited. This means new job roles in addition to lateral growth. Every step of the way, you should be having conversations about their personal and professional development, convincing them to grow with you, instead of outgrowing you.

One great way to "re-recruit" your employees is to conduct regular "stay interview" questions. What do they like about their job? What don't they like? What are they passionate about doing?

But none of this will matter if you don't recognize your top performers. Learn how your team likes to be recognized and cater to their needs. Everybody wants to feel appreciated. *Inc.com Jan. 22, 2018*

6 Ways To Work Smarter, Not Harder, And Be MUCH More Effective At Work

1. Avoid out-of-control to-do lists. When you're trying to accomplish something, whittle it down to the most essential components and throw away the rest. This way, you won't get overwhelmed.

2. Measure your results, not your time. Instead of getting bogged down with how long something is taking, track how much you're accomplishing. This will increase efficiency and reduce stress.

3. Try to keep a positive outlook. If you're helping wherever you can, pick up the slack of sick team members and never say the work is "good enough." You'll start seeing results immediately.

4. Communicate effectively. Collaborating with others is essential, regardless of the work you're doing, so strengthen these skills the same as you would with anything else.

5. Create (and stick to) a routine. The more you can build good habits, the faster you can get down and focus.

6. Stop multitasking. The data shows that people are much worse at tracking multiple tasks at once than they think. Cut out the clutter and zero in on what's important in each moment. *Inc.com Dec. 29, 2017*

Who Else Wants To Win A Fun Prize?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Jo Ann from Granite City, IL! She was the winner from the drawing of people who submitted answers for my quiz question from last month.

Who was the only Speaker of the House to later beome president?
a) Abraham Lincoln b) James K Polk c) John Adams
d) George W Bush

The correct answer was c) James K Polk! Now, here's this month's trivia question. The winner will receive a $25 Ted Drewes gift card!

What was the name of the ransomware variant that infected millions of computers around the world in May of 2017?
a) Petya b) Wannacry c) Cryptoblocker d) Gremlin

Submit your response to answer@computer-service.com! Everyone who answers correctly will be placed in the drawing to win our fun prize!