TECHNOLOGY TIMES

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

GRS TECHNOLOGY SOLUTIONS

Announcing...

REFER A BUSINESS, GET $ 250!

By recommending businesses you can help them enjoy worry-free IT and reap some REWARDS for yourself!

Because they are being referred by you, we'll extend a FREE 30-Point Problem-Prevention Network Audit to the referral, and...

We will send you or the charity of your choice a check for $ 100! If the referral becomes a client, we will give you or your favorite charity another $ 150!

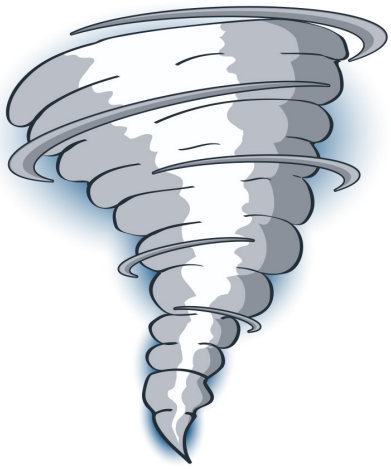
Visit: www.grstechnologysolutions.com/referralprogram or call us at (703) 854-9559 for **more information!**

7 Ways To Dodge A Data Disaster

You stride into the office early one Monday morning. you grab a cup of coffee, flip on your computer and start checking e-mail... A note pops up that rivets your attention:

"Your files have been encrypted. Send $5,000 within five days or they will all be destroyed."

You start sweating as your throat constricts and your chest tightens. Sure enough, every time you try to open a document, the same message appears. Your phone rings. It's Bob in accounting, and he's having the same problem. All files across your entire network have been encrypted. You contact the local police. They suggest you call the FBI. The FBI says they can't help you. What do you do next?



a) You pay the five grand, desperately hoping you'll get your data back, or...

b) You calmly call your IT provider, who says, "No problem, your backups are all current. No files were lost. Everything will be restored by noon, if not sooner."

If your answer is "b," you breathe a sigh of relief and get back to work as your backup plan kicks in…Ransomware attacks are more common than ever, especially at smaller companies. That's because small companies make easy marks for hackers. The average small business is much easier to hack than high-value, heavily fortified targets like banks and big corporations. According to Time magazine, cybersecurity experts estimate that several million attacks occur in the US alone every year. And that figure is climbing.

So how can you make sure you never have to sweat a ransomware attack or other data disaster? One sure solution is having a solid backup

Continued pg.2

plan in place. When all your data and applications can be duplicated you have plenty of options in the event of an attack. Here then are seven ways to make sure you're in good shape, no matter what happens to your current data:

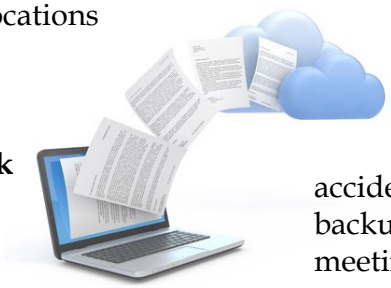
Insist on regular, remote and Redundant processes. A good rule of thumb is 3-2-1. That means three copies of your data is stored in two off-site locations and backed up at least once per day.

Don't cheap out on disk drives. Less expensive arrays that save money can leave your data at risk. Get features like a redundant power supply and hot spare disks.

Guard against human error. Make sure people doing backups know exactly what to do. Take people out of the loop and automate wherever possible. And watch for situations where backups aren't a part of someone's regular duties.

Check backup software settings routinely. When new software or updates are put into service, a change in the way the settings are configured can cause incomplete backups, or backups that fail. Do the people who maintain your backups include this on their regular to-do list?

Make sure critical files aren't getting left out. As resources are added and quarterly or annual priorities shift, documents and folders can get misplaced or accidentally left off the backup list. Insist on a meeting with your backup management team to make sure all mission-critical files are included in your organization's data recovery systems.



Address network issues immediately. Any component in your network that isn't working properly can introduce another point of failure in your backup process. Every juncture in your network, from a misconfigured switch to a flaky host bus adapter, can hurt your backups.

Ask for help with your data backup and recovery system. You cannot be expected to be an expert in all things.

Data Recovery Review Reveals Backup System Vulnerabilites

Yet data is the backbone of your business - its protection and recovery should not be left to chance. Leverage the knowledge, skill and experience of an expert who stays current with all the latest IT issues.

Data Recovery Review Reveals Backup System Vulnerabilities

Don't let your company become yet another statistic. Just one ransomware attack can result in a serious financial blow if you're not prepared.

Help us to Stop Cybercrime!

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim!

We have put togheter a FREE Executive Report "7 Urgent Security Protections Every Business Should Have in Place Now", that will get you started in protecting everything you've worked so hard to build.

To download your FREE Report, go to
www.grstechnologysolutions.com/sittingduck

Avoiding Technical Support Scams

Cybercriminals don't just send fraudulent email messages. They might call you on the telephone and claim to be from Microsoft. They might also setup websites with persistent pop-ups displaying fake warning messages and a phone number to call and get the "issue" fixed. They might offer to help solve your computer problems or sell you a software license. Once they have access to your computer, they can do the following:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software.
- Convince you to visit legitimate websites (like www.ammyy.com) to download software that will allow them to take control of your computer remotely and adjust settings to leave your computer vulnerable.
- Request credit card information so they can bill you for phony services.
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.

Telephone tech support scams:

Cybercriminals often use publicly available phone directories, so they might now your name and other personal information when they call you. They might even guess what operating system you're using.

Once they've gained your trust, they might ask for your user name and password or ask you to go to a legitimate website (such as www.ammyy.com) to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information are vulnerable

Do not trust unsolicited calls. Do not provide any personal information

Scam Pop-Ups:

Another well-known trick is the website pop-up, that little browser window that sometimes appears while you're searching the Web. Cybercriminals set up websites with scam pop-ups with messages and phone numbers. These pop-ups usually are not easy to close.
While some pop-ups are useful and important, others are traps that attempt to mislead you into revealing sensitive personal or financial information, paying for fake anti-virus software, or even installing malware and viruses onto your device.
Do not call the number in the pop-up.

How to report tech support scams:

Whenever you receive a phone call or see a pop-up window on your PC and feel uncertain whether it is from someone at GRS Technology Solutions, don't take the risk. Reach out directly to one of our technical support experts dedicated to helping you.

How to protect yourself from tech support scams:

If someone claiming to be from Microsoft tech support contacts you:

- Do not purchase any software or services.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.

Shiny New Gadget Of The Month:

Thought Oculus Was King?

Think Again

Once upon a time, Oculus Rift ruled the world…

The virtual reality (VR) world, anyway. Not so much anymore. Now that VR heavyweights Sony, HTC and Samsung have entered the ring, there's a whole new reality in, well…VR.

Sony's PlayStation VR was recently crowned "Editor's Choice" by PC Mag. And, if you happen to own a compatible Samsung Galaxy smartphone, such as the S7 or S7 Edge, you can get "untethered" VR for just $100. You'll pay four times that for the Rift, HTC's Vive or Sony's PlayStation VR – all tethered sets, requiring a clunky cable from headset to hardware.

Vive has the most advanced technology, but Rift is nearly as sophisticated and sells for $200 less. You could shell out that much for the Rift's hand controllers, but, according to PC Mag, they're well worth it. So while Oculus may not be king, it's still a serious contender.

As of January 31, "outsiders" can now Skype into the White House Press Room. This enables journalists outside the Washington, DC, area to ask questions during White House press briefings. It's part of the Trump administration's strategy to keep in touch with people outside the beltway. Journalists attending via Skype must be at least 50 miles from the DC area. All political questions aside, it's just another example of business (or, in this case, government) taking advantage of available technologies. Or, in this case, finally catching up… Skype, the world's largest video calling service, is nothing new – it's been around since 2003. Sometimes it just takes a while for users to figure out how to make tech work to their advantage. *Yahoo.com, 01.31.17*

Anti-malware programs can't even touch this new kind of attack... "Fileless" attacks became all the rage among hackers in 2016. According to a report by cybersecurity firm Carbon Black, fourth quarter 2016 saw a 33% rise in these "non-malware" attacks compared to the first quarter. Experts expect the trend to continue through 2017. Cyberbad-guys carry out these attacks in any number of ways. Their "en vogue" method at the start of 2017 was hijacking PowerShell and WMI (Windows Management Instrumentation) to do their dirty deeds. Brian Kenyon, chief strategy officer for Symantec, said recently, "Fileless infections are difficult to detect and often elude intrusion prevention and antivirus programs." Reports show the Democratic National Committee hack last year used a fileless attack. *DarkReading.com, 12.27.16*

"DIY" data security kits can offer basic protection. Are you a do-it-yourselfer willing to take defending your company's data into your own hands? If so, you can find a variety of low to no cost products that provide basic safeguards. Koozali SME Server, for instance, bundles security and other server apps for small businesses. These include file sharing, directory access, redundant backups, firewall and web hosting. Its makers claim you can be up and running with it in less than 20 minutes. It's based on Linux, yet allows you to network Windows and MacOS as well as Linux-based devices. It's all free and there is no paid version. However, because no support is provided, you may need to contact a professional for assistance. *SmallBusinessComputing.com, 12.21.16*

Client Spotlight: Congratulations to PEG 2017 ENERGY STAR Award!

We want to extend our congratulations to our client PEG who just won the 2017 Energy Star Award, which is given by the U.S. Environmental Protection Agency (EPA) and the Department of Energy (DOE), each year, to honor organizations that have made outstanding contributions to protecting the environment through energy efficiency.

ENERGY STAR AWARD 2017
PARTNER OF THE YEAR
Sustained Excellence

We understand the importance of preserving our natural resources to contribute to the future of next generations!