ISSUE 6-5

BITS & BYTES

INSIDER TIPS ON HOW TO USE TECHNOLOGY TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

IN THIS ISSUE

Do I Need To Back Up Data That's Already In the Cloud? 1
Shiny New Gadget of the Month 2
How a Small Bottleneck Can Affect Overall Performance 2
Tips To Keep Your Server Safe 3
Ways to Improve Android Battery Life 4
How To Avoid a Phishing Scam 4

MAY
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 forever."

Joe Stoll, President
Technical Action Group (TAG)
JStoll@TechnicalActionGroup.com

Do I Need To Back Up Data That's Already In the Cloud?

The computing world is forever changing. Over the last 15 years, SaaS (software as a service) providers have offered the convenience of data backup for your cloud applications such as CRM systems, SalesForce, Google Apps and Microsoft 365. The business question is, if I'm already working with a SaaS provider and my data is already "in" the cloud, do I really need to back up my data to another cloud? After all, isn't the SaaS provider doing that for me?

Well, yes and no. Yes, your data (one of your company's most valuable assets) is being backed up by the service provider. And yes, it's in the cloud. And yes, these providers have backups to their backups … but are they backing up your business-critical information? Can you guarantee that? And do you have access to it in a timely manner? The answer to these questions may be no. As a rule, SaaS providers do not open backups to customers, nor do they make restoring critical data easy or intuitive. For example SalesForce, the first commercially available SaaS application, does nightly customer backups. But if you need to recover your data, you have to go directly to SalesForce and pay a minimum of $10,000, then wait a few weeks for your data to be restored.

There's no question that the results of data loss can be devastating to your company. But when it comes down to it, it's your company information and you need to take responsibility for safeguarding it. You need to have a strategy in place.

Want to learn more about how to back up your cloud SAAS applications? Contact Joe Stoll at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com to schedule a time to discuss your particular situation and what solutions are available to you.

TAG we're I.T. Technical Action Group Inc

Shiny Gadget of the Month

SaneBox

Have you ever felt overwhelmed or even drowning with the number of emails in your inbox?

Then SaneBox could be your answer. This month's gadget is a cloud-based software application that helps you manage your email. SaneBox analyzes your email behaviour on all your devices. Then, based on which emails you let slide and which ones you open right away, SaneBox creates rules about sorting your email for you.

The result? Your inbox only has emails you need to attend to now. All other emails go to your SaneLater folder. You can drag and drop emails from that folder to your inbox, and from then on, those emails will display in your inbox.

SaneBox keeps you focused on high-priority emails. There's nothing to download. There are additional productivity features to manage tasks, your calendar, and your attachments. And the SaneBlackhole is the fastest way to unsubscribe from emails. See www.sanebox.com.

How To Get Your Staff To Produce Results

Are you struggling to find ways to make your employees more productive? Do they seem distracted by Facebook and not committed to their job or your company? In today's social media saturated world, it may seem difficult to keep your employees focused. So what can you do? Here are four ideas to get staff on your side and have them producing results.

Set clear goals

In order for your employees to produce results and reach their productivity potential, they need to know what is expected of them. At some organizations, it may be perfectly acceptable to spend one hour surfing the Internet everyday and seven hours working; or it may be considered normal to count a lunch break towards the eight hours worked. The truth is that more and more employees are bouncing between jobs from company to company, and each organization has a different set of standards and expectations. If it's not communicated to your employees what yours are, you can be certain that they'll make up their own.

Additionally, your employees need to know what results you expect them to produce. Maybe that means they need to sell a certain volume of products each month, or maybe it means they need to consistently score a four-star customer satisfaction rating. Whatever it is, your employees need to be aware of your expectations and have some sort of goal to shoot for. This gives you a way to see the results each employee is producing. Then you can try to find a solution to increase the productivity of your lower performing staff.

Be personable with your employees

Have you ever had a boss that rarely interacted with employees and that everyone feared? Maybe he stayed locked away in his office most days or ignored staff members as he quickly strode through the office never cracking a smile. Do you think employees want to produce results for a boss like this? They might, but it may be out of fear of losing their job rather than genuinely wanting to help that boss and the company at large.

Interact with your employees. And not only about work. Ask them how their weekend was. Find common interests to talk about. Take the time to get to know them. It's easy for employees to not produce results or care about their job if the business owner is unapproachable and distant. On the contrary, if the owner is personable and friendly with staff, it is harder for an employee to slack off and not commit to the company's growth. It's natural for employees to work harder for a person they know, rather than one who's "all business" and persistently unavailable.

Listen to your employees' feedback

To go along with being personable, take the time to gather and listen to your employees' feedback. If you show that you value their opinions, they'll feel part of the team and organization. When this happens, they'll be more committed to your goals and will want to see the company succeed as much as you do.

Of course that doesn't mean you need to take every bit of employee feedback and run with it – it simply means keeping an open mind. Your team will respect you more and work harder for you as a result.

Provide reliable equipment

This is a no brainer. But if an employee doesn't have the reliable equipment and tools to complete their job, their productivity levels will plummet. A broken computer, crashed server or faulty Internet connection will have your staff twiddling their thumbs and playing with their phones in no time. If it's your technology that's the culprit in this situation, Managed Services represent an exceptional solution to prevent your IT from ever breaking down in the first place. What does that mean for your staff? Less downtime, more productivity and more results.

Interested in discovering more ways to boost employee productivity? Want to learn how Managed Services can ensure the reliability of your IT and prevent downtime? Contact us.

Tips To Keep Your Server Safe

Your Server Is The Heart Of Your Business Network. When something goes wrong, you lose access to key resources while productivity, customer service, and your bottom line suffers. Here are a few things you may be forgetting that could be compromising your server's security.

Back Up Your Server. While most businesses understand the necessity of backup up their important documents and files, many don't think to create a backup of their entire server. Without a complete image of your server, all of the software, permissions, and server settings will be lost in the event of a server crash. Avoid this by using imagine software to create a complete image of your server's installed software, settings, permissions, printer configurations and much more.

Test Your Backup. Many companies that have a server backup system in place don't test the backup process and often find out too late that the system is not working as it should be. Scheduling periodic tests for your backup system is a wise investment of time and resources. If you have an image backup system as described above, you should also test the entire system restore process to be sure it is working as expected.

Configure Server Security Settings. Many businesses have a single set of administrator permissions setup on their servers. This means everyone in the company can potentially access financial records, social security numbers, salary information, and additional sensitive data from other employees. The best practice is to set up a tiered permission structure, giving access to each user based on what they need to know.

Perform Regular Updates. One of the best things you can do to ensure the security of your server is to download and install operating system and software updates on a monthly basis. Failure to do this leaves your server open to vulnerabilities that hackers can exploit to gain access to your system.

Use a Reliable Battery Backup. A commonly overlooked area of server security is the addition of battery backup. Battery backup systems are inexpensive and usually provide five to ten minutes of power during an outage. If the power is out longer, the server will shut itself down properly and gracefully, performing all necessary functions to keep your data safe.

A bit of foresight goes a long way to keep your server safe—so don't wait to implement security measures. The most expensive disaster is the one you're not prepared for!

Have more questions about server security? Call Joe Stoll at 416-489-6312 x 204!

Tip of the Month: 3 Ways to Improve Your Android's Battery

We all know how useful smartphones are, especially when you're in a pinch and need to access the Internet. However, you can't take advantage of any of these sweet features if your battery dies out within four hours of a full charge. This might be an extreme case, but the point stands that there's a ton of stuff draining your battery when you don't want it to.

According to CNet, there are several ways you can cut down on the amount of battery life that's wasted throughout the day. Most of them involve disabling certain features that are innately made available on mobile devices.

Disable Unused GPS-Based Services

By default, your phone has its GPS enabled. As you can imagine, all of the communication between satellites, cell phone towers, and the phone's GPS chip put a ton of strain on your device's battery. However, some of these GPS-based services aren't really required for you to enjoy all of the benefits of a smartphone. These two, according to CNet, are Location reporting and Location history. These settings use your phone's GPS alongside other Google applications to enhance your user experience, but they aren't really necessary. Disable them by going to **Settings > Location > Google Location Reporting.**

Cont'd on Back Page...

How a Phishing Scam Works And What You Can Do To Protect Yourself

Most hacking attacks are the result of a flaw or vulnerability found within the code of a program or operating system, but we rarely take into account the ones that don't. Hackers often take advantage of the human side of hacking as well, a process known as "social engineering." This is usually the act of conning users into handing over personal information of their own free will, and it's surprisingly effective.

As you can imagine, social engineering involves exploiting the people who work with the technology rather than the technology itself. This particular method allows those who might not be as tech-savvy (or those who aren't particularly known for their common sense) to obtain important information, like passwords or dates of birth, from unsuspecting foes. Those who are more skilled with technology can perform more elaborate social engineering attacks, like replicating websites to infect systems with malware upon visitation, or download infected software.

The most well-known social engineering hacking attack comes in the form of a phishing attack. These are typically the type of emails which appear to be the genuine article from an institution you might have relations with, such as a bank. These emails request that you update or confirm your personal information. It can be difficult to discern these from the real deal at times.

Other, more focused attacks are called spear phishing attacks. These are designed to target a specific individual, or multiple specific targets. Sending emails personalized to get users to fork over financial information, or even going to lengths such as contacting your business posing as someone from a media outlet.

According to HowToGeek.com, this method isn't limited to being used remotely. Social engineering hackers can also get up close and personal with their attempts:

An attacker could walk into a business, inform the secretary that they're a repair person, new employee, or fire inspector in an authoritative and convincing tone, and then roam the halls and potentially steal confidential data or plant bugs to perform corporate espionage. This trick depends on the attacker presenting themselves as someone they're not. If a secretary, doorman, or whoever else is in charge doesn't ask too many questions or look too closely, the trick will be successful.

How To Prevent Social Engineering Attacks

In the end, keeping your business safe from social engineering attacks comes down to identifying them from the genuine article. In order to minimize the risk of falling prey to these hacks, keep these tips in mind.

Some suspicion is better than none at all. If you're receiving strange emails, messages, or phone calls from users you don't recognize, it's best to be on the safe side and not respond until you're sure that you're dealing with the real deal. It's better to call the institution at the number you have on record before handing over any information you feel is suspicious. If something seems suspicious, such as poorly worded emails and strange links, it's best to question it.

Avoid links in emails to websites which gather sensitive information. These websites could be fake phishing sites designed to look like the official institution website. For example, you receive an email asking to update your bank information, and the link leads to a sign-in form. This is a fake site designed to fool you into entering your credentials. In this case, it's best to try logging into the official site rather than through the email. Look at the URL and scan it for subtle differences which might hint at trickery.

Enable spam and phishing filters for your email and browser. Some browsers have built-in phishing and security filters, which should always be active. These can prevent your employees from accessing a known phishing site. One particularly powerful solution is TAG's Unified Threat Manager (UTM). This solution equips your business with everything it needs to keep outside threats from getting into your network, including spam filtering and web content blocking.

....cont'd : 3 Ways To Improve Your Android's Battery Life

Make Sure WiFi-Scanning Is Turned Off

You might use WiFi in the office or at home, but what about when you're out and about, on the open road? Most of the hot spots you encounter in public won't be safe for you to connect to reliably, so it's best to turn off auto-connecting to WiFi on your device. However, even when you're not connected to WiFi, your device will search for connections unless you tell it not to. You can make sure this setting is off by following WiFi settings > Advanced. If the WiFi scanning box is unchecked, you're all set.

Control Your Data Sync

You might notice how your Android smartphone is constantly syncing to your Google account. This is a good sign that you're keeping the files on your phone backed up online and ready to go in the event you lose data. However, this also means that your phone's battery is draining due to it constantly syncing to the Google account. Instead of turning off the sync for all of your accounts, you can limit what syncs and what doesn't. Do this by heading to Settings > Accounts. Select the account to access the sync settings. You can then uncheck any items you don't want synced, or turn it off completely if you want.

These are only three ways out of many to limit how much battery life your Android device consumes.