ISSUE 8-11

BITS & BYTES

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

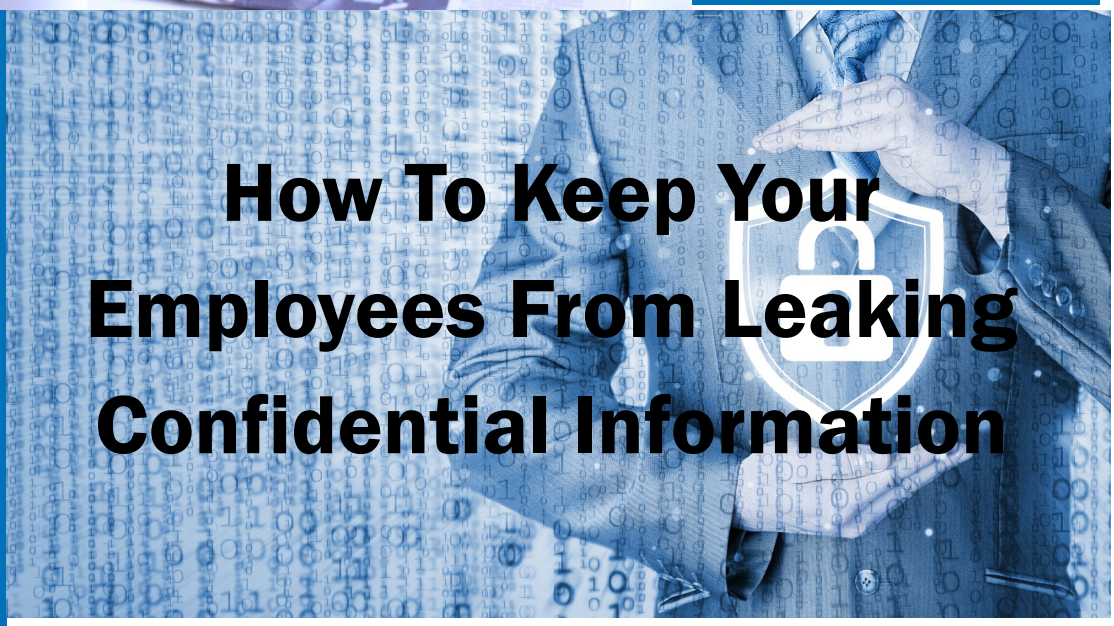
IN THIS ISSUE

November 2017

"TAG specializes in providing management level responsibility for all the technology in your business. This includes support for your network and working with other hardware & software vendors who's technology you use.

We do this with friendly, proactive & responsive service!

Joe Stoll, President
Technical Action Group (TAG)



How To Keep Your Employees From Leaking Confidential Information

Back in 2014, Code Spaces was murdered. The company offered tools for source code management, but they didn't have solid control over sensitive information — including their backups. One cyberattack later, and Code Spaces was out of business. Their killer had used some standard techniques, but the most effective was getting an unwitting Code Space employee to help — likely via a phishing attack.

When it comes to cybercrime that targets businesses, employees are the largest risks. Sure, your IT guys and gals are trained to recognize phishing attempts, funky websites, and other things that just don't seem right. But can you say the same thing about the people in reception, or the folks over in sales?

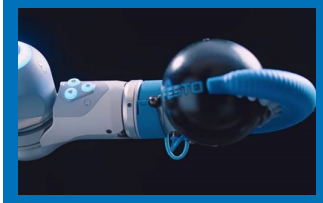
Sure, those employees might know that clicking on links or opening attachments in strange emails can cause issues. But things have become pretty sophisticated; cybercriminals can make it look like someone in your office is sending the email, even if the content looks funny.

It only takes a click to compromise the system. It also only takes a click to Google a funny-looking link or ask IT about a weird download you don't recognize.

Just as you can't trust people to be email-savvy, you also can't trust them to come up with good passwords. It may sound so 2002, but plenty of people still use birthdays, pet names, or even "password" as their passcodes — or they meet the bare-minimum standards for required passcode complexity. Randomly generated passcodes are always better, and requiring multiple levels of authentication for secure data access is a must-do.

Remember, that's just for the office. Once employees start working outside of your network, even more issues crop up. It's not always possible to keep them from working from home, or from a coffee shop on the road. But it is possible to invest in security tools, like email encryption, that keep

Shiny New Gadget Of The Month:



OctoGripper, the Octopus-Inspired Robotic Arm, Is Here

The animal kingdom is a reliable place to turn for mechanical inspiration. The German automation company Festo just made a robotic arm that takes its cue from an octopus. Meet the OctoGripper!

Festo figured it's hard to beat the octopus' flexibility. Built with a soft silicone structure that can be pneumatically controlled, the device bends inward to grip an item with two rows of suction cups. These create a vacuum, allowing the gripper to hold onto objects tightly while moving quickly - a common challenge in robotics.

This isn't the only thing Festo is taking from nature. They want to see the OctoGripper incorporated into their BionicMotion Robot, which is inspired by an elephant's trunk. These could work side by side with humans, perhaps speeding up work.

Or they could pair up with Boston Dynamics and start the best robotic zoo this side of "Horizon: Zero Dawn."

data more secure if they have to work outside your network. And if people are working remotely, remind them that walking away from the computer is a no-no. Anybody could lean over and see what they're working on, download malware or spyware, or even swipe the entire device and walk out — all of which are cybersecurity disasters.

When it comes to cybercrime that targets businesses, employees are the largest risks.

Last but not least, you need to consider the possibility of a deliberate security compromise. Whether they're setting themselves up for a future job or setting you up for a vengeful fall, this common occurrence is hard to prevent. It's possible that Code Space's demise was the result of malice, so let it be a warning to you as well! Whenever an employee leaves the company for any reason, remove their accounts and access to your data. And make it clear to employees that this behaviour is considered stealing, or worse, and will be treated as such in criminal and civil court.

You really have your work cut out for you, huh? Fortunately, it's still possible to run a secure -enough company in today's world. Keep an eye on your data and on your employees. And foster an open communication that allows you to spot potential — or developing — compromises as soon as possible.

Nagging Reminder: Reboot Your Computer Nightly!

If you've been a client of TAG's for a while, odds are you (or someone in your company) has been asked by one of us when was the last time you reboot your PC when you call in with a report of a slow PC. There are often telltale behaviours with a PC that are caused by it not being shut down for days or weeks on end, which a quick reboot can often fix.

Turning off your PC at night has an obvious benefit: it saves electricity. Rebooting your PC, on the other hand, has less obvious benefits. Most laptops have the ability to go into sleep mode, which makes it easier to skip rebooting. Even though improved operating systems and more efficient computers have made rebooting less necessary, it still has advantages

Flushes RAM Your computer's random access memory (RAM) is also known as volatile memory, because it's constantly in flux -- as opposed to solid-state memory, such as your hard drive. Your RAM handles lots of different short-term tasks and data, like running processes and holding program values. Rebooting your computer flushes out all this information, allowing your device to start anew and helping it run faster and more efficiently.

Fixes Small Errors Many computer users are unaware that when they reboot, it runs diagnostics on itself, automatically fixing minor errors. These errors can range from buggy or glitchy applications to problems with the RAM. This is why you'll often find that when your computer freezes, or has a problem you don't know how to fix, simply restarting resolves the issue.

Stops Memory Leaks
Memory leaks occur when a program doesn't close properly. Every program that runs on your computer uses memory (usually RAM) while it's open. When you close the program, that memory should return to your computer. Outdated, overused or glitchy programs, however, can have memory leaks, which occur when memory isn't returned to the computer. Rebooting your computer each night can help prevent memory leaks from occurring.

And if the above is still too "geek speak" for you, just think of it this way. If you never turned your car off when you drove it home, wouldn't it get pretty tired and worn out and cause all sorts of problems? Computers, like cars, and people, need breaks too. Now if we humans only had a reboot button for ourselves...

Goal Setting Doesn't Work

(And Santa Claus May Not Exist)

When we were kids, we thought we could write down a list of everything we wanted and mail it to the North Pole. When we grew up, we realized there wasn't really a big roly-poly guy who delivered presents. A real person had to earn the money, march through shopping malls, wrestle the presents home, wrap them up, and place them under the tree. But I think many people still believe in Santa Claus. Why else would they write down a list of wants on New Year's Day, stick it in a drawer for the rest of the year, and wait around for their lives to change?

Sorry, but it's time to grow up. Most people know how to write down goals, but few ever achieve them. Want to stop chasing rainbows, wishing on stars, and rubbing lamps, and instead achieve real results? This article will help you start.

WARNING: Achievement requires work, discipline, commitment, and maybe some heartache and a stiffened spine. If any of that makes you queasy, I invite you to continue reading.

The Cause of All Your Problems — and the Solution

When I ask people what they want to improve in their lives, I hear things like, "I need to make more money," or "My marriage is unhappy," or "I need to lose weight."

But these are simply symptoms or outcomes of the problem. The cause of the problem is you — and this is probably one of the most sobering understandings you can reach as you work toward your stated goals. Whatever it is you want to change, whether it's your marriage, financial situation, or weight, you'll never achieve lasting change until you change. Once you improve, everything else around you will improve.

In life, you don't get what you want; you get in life what you are. The success you have in life correlates with your level of self-worth. But the human tendency is to engage in the study of effects, while giving little attention to causes.

I see this travesty play out every day. People complain about their terrible marriage, so they leave it. Oddly enough, they end up with similar problems in the next relationship. Why? Because they didn't address the real problem. The same set of circumstances and patterns of behavior will create the same outcome. Some people go from diet plan to diet plan, losing weight and then gaining it all back. Why? Because the plan and the weight aren't the issues or the solutions; they are effects, and the weight will ultimately meet them back where they are.

If Your Parents / Aunts / Uncles / Use a Computer, Have Them Take This Quiz To Keep Them Safe From Being Scammed

More than 3 out of every 5 American and Canadian seniors have been the target or victim of an online scam, according to a 2016 Home Instead, Inc. survey.

Thanks to the website www.protectseniorsonline.ca there are easy to understand resources to learn how seniors (or anyone, for that matter!) can help protect themselves from becoming a scam target.

Share the information with your family and friends to help them stay safe too.

Start by quizzing yourself to see how well you can spot an online scam.

www.protectseniorsonline.ca/

Darren Hardy is the visionary force behind SUCCESS magazine as the Founding Publish-er and Editor, and is the New York Times and Wall Street Journal bestselling author of what has been called "the modern day Think and Grow Rich": The Compound Effect—Jumpstart Your Income, Your Life, Your Success (www.TheCompoundEffect.com) and the world-wide movement to onboard 10 million new entrepreneurs through his latest book The Entrepreneur Roller Coaster--Why Now is the Time to #JoinTheRide (www.RollerCoasterBook.com). Access Darren: www.DarrenHardy.com and get free daily mentoring: www.DarrenDaily.com

How a University Campus Is Using This New Technology to Keep Its Students Safe. Remember when you got locked out of your dorm building back in college and had to wait for someone to go in or out? Those days may be gone, if new technology out of China has anything to say about it. Dorms at Beijing Normal University are being fitted with face recognition software, which will let residents in — and keep intruders and other unwanted people out. *Mashable.com – May 23, 2017*

You Won't BELIEVE Where Hackers Are Hiding Malware Now. If you use Popcorn Time or VLC, listen up: Hackers are targeting your subtitles. Yes, that's right — from bad kung fu movie dubs to the latest and greatest European cinema, this technique hides malware in the downloaded subtitle information for a movie. Once it's in your computer it takes root and communicates with the attacker. By the intermission, your machine belongs to them! If you're a Popcorn Time user, you can download the patch online. VLC and other media players should have the problem patched by the time of printing. Or, you know, you could just not download movies from the internet … but we all know how likely that is. *Techcrunch.com 5/24/2017*

Should You Have a Mobile App For Your Business?

One of the great things about apps is that you don't need to be a big developer or company to build one. In fact, according to www.smallbusinesscomputing.com, 42 percent of small businesses in the United States have their own mobile app. By the end of the year, that figure is expected to hit 67 percent! Somewhat unsurprisingly, the most cited reason SMBs said they decided to build mobile apps is to increase sales (39 percent), followed by improving customer service (30 percent). Others turn to mobile apps as a competitive advantage in specific markets (22 percent) while for some organizations, their parent company suggested an app (10 percent). But with apps becoming more affordable than ever, there are lots of reasons to invest in your own app - and lots of ways to recoup that investment. What would your ideal app do?

SmallBusinessComputing.com March 09, 2017

This Genius Debit Card Lets Parents Control Their Teenagers' Spending If you feel like your teen views you as a walking ATM machine, startup company Current might be able to help. Their new app — also called Current — allows you to track and control your teen's spending through the company's debit card. Current offers a series of robust services designed to teach your child financial responsibility while still letting them have some say over how and when they spend their money. You can set up daily spending and withdrawal limits, but you can also set up contingencies — money that's freed up, say, when chores or tasks are completed.
Techcrunch.com 5/9/2017

Your Best Employee WILL Quit ... Are You Prepared?
Employee churn is a fact of business. It's important to take steps to ensure that regardless of an employee's importance, their loss won't be catastrophic. Consider everyone on your team. If they left, what would it do to your business? Make sure to document indispensable knowledge. In the end, you should keep your team as happy as possible, but be supportive if they make the decision to leave.
Groovehq.com 12/10/15

Your Copier Is Spying On You
It may sound paranoid, but it's true: the machines you use every day around the office could be spying on your data. Copiers and multifunction printers, particularly, are some of the leading causes of business data breaches. When you consider it, it makes sense. They're among the only devices on the network that rarely have their default password changed. But these advanced copiers and printers often house images of all the pages they've ever scanned on an internal hard drive, making them the perfect target for thieves. Make sure to change the password from the default on every network-connected device in your office. This one simple step can save you a costly headache down the road. *intellisystems.com 01/31/2017*

NEVER Throw Your Boarding Pass Away, Not Even After Your Flight Everybody knows that a boarding pass is mandatory in order to board a plane. While we're in the airport, we keep a close eye on our boarding passes, clutching them in our hands like they're precious gems. But after we land, pretty much everyone ditches the ticket, whether it's lost on the floor, compacted in the washing machine or thrown directly into the trash.

This may seem innocent enough, until you realize the abundance of personal information encrypted on your pass. You'd be amazed at the information a person can glean just by scanning the QR code on the ticket: your home and e-mail addresses, your phone number and even your bank information! When you get rid of your next boarding pass, shred it. Your bank account will thank you.
LuxuryAndGlamor.com 2/5/2016