ISSUE 8-1

BITS & BYTES

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

IN THIS ISSUE

January 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)

3 "Must-Do" IT Resolutions for 2017

Happy New Year to my valued clients and readers of Bits & Bytes! I hope your holidays were fun-filled and relaxing, and that 2017 is off to a great start personally, and in business.

With a new year, brings, unfortunately, a continuation of the proliferation of security dangers for any business relying on technology. We at TAG continue to have our tech-dukes up ready to take on another year of protecting our valued clients from havoc-wreaking cybercriminals.

Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today." That's what *The Evolution of Ransomware*, a study by Mountain View, California-based cybersecurity firm Symantec, reported recently.

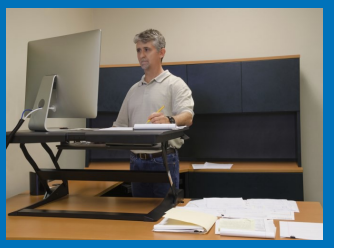
If you have any illusions that your company is safe from cyber-attack in 2017, consider just a few findings stated in a recent report by the Herjavec Group, a global information security firm:

- Every second, 12 people online become a victim of cybercrime, totaling more than 1 million victims around the world every single day. WOW.
- Nearly half of all cyber-attacks globally last year were committed against small businesses. This doesn't surprise me, as small businesses are a growing sector of the economy, and often the least protected.
- Ransomware attacks rose more than an astonishing 300% in 2016.
- The world's cyber-attack surface will grow in order of magnitude larger between now and 2021.
- The US has declared a national emergency to deal with the cyberthreat.
- There is no effective law enforcement for financial cybercrime today.

Clearly, your company's information and financial well-being are at greater risk than ever in 2017. And you cannot count on the federal or provincial government or local police to protect your interests. That's why I STRONGLY SUGGEST that you implement the following resolutions starting TODAY.

Resolution #1: Tune up your backup and recovery system. The #1 antidote to a ransomware attack is an up-to-date backup copy of all your data and software. Yet managing backups takes more than just storing a daily copy of your data. For one thing, if your business is at all typical, the amount of data you store grows by 35% or more PER YEAR. If your data management budget

Shiny New Gadget Of The Month:



Your Desk Is Killing You: Do This Instead

.
The evidence is piling up that sitting all day is bad for your health. Though not perfect, Varidesk offers a compelling solution.

On the plus side, The Varidesk sets up right out of the box – no assembly required.

With its weight-balancing system, you don't need any hardware to fasten it to your desk. And it features an attractive, sturdy design.

You can lean on it and your monitor won't go crashing to the floor. Springs and levers make it easy to raise or lower it to one of 11 preset levels.

The main flaw is that when you raise it, it also moves forward – a problem if you're in a tight space. All in all, though, it's worth looking at, especially if you have a wireless keyboard and mouse – and enough space in your office or cubicle to back up a bit.

Resolution #2: Harness the power of the cloud—but watch your back. Huge productivity gains and reduced costs can be achieved by making full use of the cloud. Yet it's a double-edged sword. Any oversight in security practices can lead to a breach. Here are two things you can do to harness the cloud safely:

⇒ ***Determine which data matters.*** Some data sets are more crucial to your business than others. Prioritize what must be protected. Trying to protect everything can take focus and resources away from protecting data such as bank account information, customer data and information that must be handled with compliance and regulatory requirements in mind.

⇒ ***Select cloud providers carefully.*** Cloud vendors know that data security is vital to your business and promote that fact. Yet not all cloud vendors are the same. You can't control what happens to your data once it's in the cloud, but you can control who's managing it for you.

Resolution #3: Set and enforce a strict Mobile Device Policy. As BYOD becomes the norm, mobile devices open gaping holes in your network's defenses. Don't miss any of these three crucial steps:

⇒ ***Require that users agree with acceptable-use terms before connecting to your network***. Be sure to include terms like required use of hard-to-crack passwords, conditions under which company data may be "wiped" and auto-locking after periods of inactivity

⇒ ***Install a Mobile Device Management System on all connected devices.*** A good system creates a virtual wall between personal and company data. It lets you impose security measures, and it protects user privacy by limiting company access to work data only.

⇒ ***Establish a strong protocol for when a connected device is lost or stolen.*** Make sure features that allow device owners to locate, lock or wipe (destroy) all data on the phone are preset in advance. That way, the user can be instructed to follow your protocol when their phone is lost or stolen.

Free Network And Security Audit Resolves Your Biggest Data Security Problems and Makes Your Systems Run Like A Fancy Swiss Watch

Ever asked yourself why some business owners and CEOs seem so blithely unconcerned about data protection?

Don't let their ignorance lull you into a false sense of security. If you've read this far, you are smart enough to be concerned.

Call Joe Stoll right now at 416-489-6312 x 204 or e-mail him at JStoll@TechnicalActionGroup.com and we'll send one of our top network security experts over for a FREE Network and Security Audit. It's your best first step to a safe and prosperous 2017.

At The Office: Be The Adult In The Room

There's a reason people refer to the office as a "sandbox," because some folks refuse to act like adults. And, if the level of childish behaviour rises to tantrum pitch and the culture becomes toxic, there's no chance for communication or growth. But the office is not a playground, and we're not children. So it's important that we enter into an "adult agreement" when we walk through the doors at work and begin our day.

When I work with companies looking to improve their business, one of the things we start with is our adult agreement. It informs the work we do for the entire day, and hopefully beyond.

Here are three agreements to make sure you're acting your age in the workplace:

Don't shoot each other down.
When a colleague brings an idea to the table – even if you disagree with it – don't shut them down just to be "right." If we want to be collaborative, we've got to consider that those around us have something valuable to offer. If you make it a habit to cut people off or discount what they're saying out of hand, you'll not only guarantee that they won't share their ideas with you again, but you'll likely miss out on insights that could help you and your company.

Own up to mistakes and bring them to the table.
Nobody is perfect – not you, not me, not Bill Gates or Mark Cuban or anyone you might admire in business. We all make mistakes, and the worst thing we can do is deny that they exist. Instead, own up to your mistakes and let everybody know what they are. We only grow and learn when we're vulnerable with each other. Admitting error is often considered a risk, but it's really an opportunity. Our mistakes let others understand who we are, what risks we're willing to take and what lessons we've had to learn. Share freely to engender trust and understanding among your teammates.

Don't hide problems.
Maybe you want to stay focused on the positive and don't want to highlight "problems." Wrong. You're not a negative person just because you bring problems to light or point out conflicts where they might exist. More likely, you're finally saying what everyone else is thinking and is afraid to say. Or you're bringing something up that's important for everyone to understand in order to improve and move forward. Put problems up for discussion and brainstorm solutions. Hiding problems only makes them grow.

As you seek to master these three steps, remember one more thing: adults don't crush each other just for acting like adults. We've got to support each other in our efforts to be truthful and vulnerable. A team is only as strong as its weakest link, so it's critical that we lift each other up. When we act like adults – especially in the sandbox – we all win.

Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success and coaching them past the excuses. After all, as he tells his clients, 100% annual growth is only 2% growth every week. It's not easy. But possible. Andy learned how to build great organizations by building a great business, which he started in college then, grew into an Inc. 500 multi-million dollar national company that he successfully sold and exited. He founded Petra to pass on to other entrepreneurs, business owners and leaders the principles and practices he used to build his successful enterprise, which are rooted in the Rockefeller Habits

Use Facebook Live To Give Your Business Personality

Using Facebook Live is dead simple.

If you haven't already, install the Facebook app on your smartphone.

Open it up, tap the red "Go Live" icon and you're on. It tells you how many are watching, plus their names and comments.

When you're done, it saves to your Timeline.

And, unlike Snapchat or Periscope, it doesn't disappear after just 24 hours.

You can share, embed, Tweet – or delete – to your heart's content.

And you can filter who sees it. As for content? Interview key employees, big shots in your niche or your customers.

Share how you're making a new product.

Or how your team relaxes. Why do it? Your customers love getting that little peek "behind the scenes."

-PostPlanner.com

"From" E-Mail Spoofing: How Spammers Send Email That Looks Like It Came From You

By now, you have probably already heard of (if not been directly affected by) email spoofing or ghosting. Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source.

A common question we get at TAG when this happens is "how do they do it? How do they gain access to my email account to spoof me"?

The answer? They don't. In fact, I'd say that 99.99% of the time it has *nothing at all to do with your account*, and your account is quite safe.

They only need your email address.

While your email *account* and your email *address* are related, they are not necessarily the same thing.

Accounts versus Addresses

Your **email account** is what you use to log in and gain access to the email you've received. In most cases, it's also what you use to log into in order to be able to send email.

Your **email address** is the information that allows the email system to route messages to your inbox.

The two are related only to the extent that email routed to you using your email *address* is placed into the inbox accessed by your email *account*.

"From" spoofing by spammers is done by creating an email account in an email program using their own email *account*, while specifying someone else's email *address*. Reputable email clients like Microsoft don't actually support this capability, or it doesn't facilitate spoofing anonymously. Not only that, but spoofing is illegal.

Spammers don't care, and bypass all that. They use so-called "botnets" or "zombies" which act more like full-fledged mail servers than mail clients (Microsoft Office Outlook, and so on). They completely bypass the need to login by attempting to deliver email directly to the recipient's email server. It's pretty close to being anonymous, as the spam is exceedingly difficult to trace back to its origin.

There's nothing special about the "From:" address. It's just another field which, like the "To:" field, can be set to any value you like. By convention – and sometimes automatically – we set it to our own email address when we send mail, so that we get any responses. But there's nothing that says it has to be that way.

And often there's nothing that forces it to be that way.

Similarly, since it's just a setting on outgoing email, seeing a particular "From:" address doesn't imply any relationship to the actual account that would receive email that is sent to that address. Spammers don't need access to the account to make it appear in a "From:" line – all they need to do is effectively to type it in the "From:" line. Nothing more. That spam didn't really come "From:" that address at all.

Want Better Collaboration At Work? Play These Tunes!

Research has already shown that teams who listen to music together at work feel more bonded and collaborate better.

Yet playing music in the office begs the question – what type of music do you listen to?

It's a topic likely to end up in wrangling and conflict.

However, a recent study at Cornell University offers a scientific answer.

And, while metal fans may not be thrilled with it, the results weren't exactly shocking. The study found that people who listen to happy music were more likely to cooperate, regardless of age, gender or academic major, than those who listen to unhappy music. Interestingly, they found it was not the vibe, but the bouncing beat, that gets teams in sync. *-Inc.com*

At TAG, our Bose SoundLink Mini Bluetooth Speaker plays tunes all day long, with team members taking turns playing "DJ for the Day" using iTunes on their phones. But there's always consensus on the type of music so no one's ears bleed listening to music they don't like!