ISSUE 6-10

BITS & BYTES

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

IN THIS ISSUE

October 2015

"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)

When Your Web Developer Needs To Be Watched VERY Closely By Your IT Guys

Last week saw my incredulous frustration at yet ANOTHER case where a client's web developer who was moving our client to a new website, took down their email during the process, leaving our client without mail for FIVE hours, all of those during the workday. For email dependent businesses (as was our client), this duration of an outage can HURT your business in countless ways.

In the developer's defense he didn't do it intentionally, however this occurred because he made changes on the DNS (essentially the telephone directory on the internet) without understanding the ramifications of the changes he made.

Here's what happened (in plain English): While doing his work to move the client from the current website to the new website, he ended up resetting the DNS records to point to the new website and as well, had the records for email delivery pointed to the new website. This should NOT have been done and as a result this caused my client's mail flow to stop.

We became aware of the mail stoppage from our monitoring system that alerted us that there was an issue with mailflow, and we alerted our client immediately. We quickly investigated the root cause for the stoppage and learned that the mail identifi- one domain to another were changed by the web developer. This was done in error while he was trying to bring our client's new website live.

HOW TO AVOID THIS

Make sure that your web developer does not have login privileges to the location where the DNS entries for your domain are managed. If he or she asks for them, don't provide them unless these credentials are the same ones that they need for managing the website files (some web hosting companies have one username and password to manage files and DNS). If he asks for the credentials for DNS, don't provide those. Instead, have the developer send a written request to TAG's Help Desk (or your IT provider), clearly stating the changes that are needed to effect the move or launch of the website. Having TAG involved will ensure that there is no mail flow disruption because we are trained on how to make DNS changes properly, and validate once completed.

©Jeff Stahler/Distributed by Universal Uclick for UFS via CartoonStock.com

Shiny New Gadget Of The Month:

The Amazon Echo: Like Siri For Your Home

It's not Rosie the Robot, but your first voice request to Amazon's new Echo moves you one step closer to living like the Jetsons… Think of it as a plugged-in version of Apple's Siri or Microsoft's Cortana.

This "smart" speaker in a 9¼ x 3¼-inch cylinder can order products, turn off lights, set a timer, look up and give you sports scores, read you a book from Audible and more. You might even get it to tell you terrible jokes… It won't replace a high-end stereo, but its sound quality compares with any Bluetooth speaker, and it can fill a good-sized room in your home. Bottom line: Echo offers hands-free, at-home audio access to just about anything on the web, with better sound than a smartphone or tablet.

All in all, it can make your life easier. And maybe just a little more fun.

Cybercriminals Now Have a Bull's-Eye On Small Business...Is YOUR Company's Data At Risk?

In a December 2014 survey by the National Small Business Association, 61% of small businesses reported being victims of a cybercrime within the past 12 months.

The average cost to recover from a cyber-attack skyrocketed from $8,699 per attack in 2013 to $20,752 per attack in 2014. And, of the businesses targeted, 68% said they'd been hacked more than once.

Experts agree, as cybercrooks become ever more sophisticated, the threat to small businesses is going to get worse before it gets better…

So what can you do to beat the bad guys?

Here are three common ploys used by hackers – and how you can fend them off:

Phishing – A really legitimate-looking e-mail urges you to click a link or open a file that triggers a malware installation on your computer.

> **Best Defense:** Don't let anyone in your company open files or click links in an e-mail unless they're certain who it came from.

Cracking Your Password – Hackers can run programs 24/7 testing password combinations. The easier your password is to guess, the more likely it is they'll crack it.

> **Best Defense:** Consider using a password manager that generates and stores tough-to-crack passwords. For extra security, use unique passphrases for financial accounts in case the manager gets hacked.

Drive-By Download – You visit what appears to be an innocent site; yet when you click, your device gets hacked – and you may never know it, until it's too late.

> **Best Defense:** Make sure your browser is up-to-date, or use one that updates automatically, such as Firefox or Chrome. Internet Explorer users have been found to be most vulnerable to these attacks, if IE is not being updated. Part of TAG's monthly Windows update / patching process, updates the IE version for its clients on a managed services plan.

Unfortunately, these three examples are just a small sampling of the dozens of ever more ingenious ways cybercriminals are breaking down the doors and destroying unprepared businesses.

Let us help! Through November 30th, call our office and receive a FREE 15-Point Cyber-Security Audit to uncover gaps in your company's online security.

One of our senior IT pros will come to your office and conduct this comprehensive audit. We'll then prepare a customized "Report Of Findings" that reveals specific vulnerabilities and a Prioritized Plan Of Attack for getting any problems addressed fast.

To take advantage of this limited-time offer, just call Joe Stoll at 416-489-6312 X 204 or email him at JStoll@TechnicalActionGroup.com to schedule yours today!

Do You Accept Credit Cards?
Watch Out For These 5 Pitfalls That Could Lead to Lawsuits

If your company is not fully compliant with Payment Card Industry (PCI) Security Standards, you could be at risk of a serious tangle with attorneys. Technically, PCI guidelines are not a hard-and-fast set of laws. However, merchants can still face hefty liabilities for not meeting them. Avoid these mistakes to keep your company out of hot water with attorneys:

1. Storing Cardholder Data In Noncompliant Programs

Many states have laws regarding data breaches and, depending on where you accept cards, you may be subject to many of them. For example, Massachusetts has 201 CMR 17.00, which requires companies keeping any personal data from Massachusetts residents to prepare a PCI-compliant plan to protect that data. If a company then fails to maintain that plan, the business may face state prosecution.

2. Fibbing On The Self-Assessment Questionnaire

If you have considered tampering with the reports from your company's Approved Scanning Vendor, think again. Time invested now to fix any holes in your data security system could save you big-time from the penalties your company could suffer if there's ever a data breach.

The same thing applies to simply "fudging the truth" on self-prepared compliance reports. Even if you think it's a harmless stretch of the truth, don't do it.

3. Not Using The Right Qualified Security Assessor

Many companies use Qualified Security Assessors to help them maintain their PCI compliance. Every QSA does not necessarily know as much as another, however. It's important to select someone who both understands your business and stays up-to-date on the latest version of PCI Security Standards.

4. Trying To Resolve Data Compromises Under The Radar

You may be tempted to fix a customer's complaint yourself if they inform you of a data compromise. Not informing credit card companies of data breaches, however small, can lead to you no longer having access to their services. Those credit card companies can then file suit against your company, costing you big bucks in the end.

5. Not Checking ID For Point-Of-Sale Credit Card Use

Sometimes it seems like no one checks IDs against the credit cards being used, so merchants tend to be lax about doing so. Unfortunately, running just one unauthorized credit card could cost you a lot in the long run.

Even if the province in which you do business does not have specific laws regarding PCI compliance, a civil suit may come against your company for any data breaches. The court will not favor you if you have not been PCI-compliant.

All in all, it pays to pay attention to PCI compliance – a little time invested today could save you big-time tomorrow.

TAG is well-versed on the requirements for a company to become PCI compliant in Canada, and has helped many clients get there. If you keep credit cards on file, give Joe Stoll a call today. He'll guide you through what's required.

Comparing Managed IT Services & Break-Fix Plans

When it comes to IT services, there are two types of service plans that most IT companies offer. The first is "***Time and Materials***" (known as "Break-Fix"). The second is "***Managed IT Services***". But which is best for your business?

Time and Materials

Under this model, you pay an agreed upon hourly rate for a technician to fix computer issues when something breaks. The scope of work under this model can be to resolve a specific problem (like removing a virus) or a large project like performing a network upgrade.

Managed IT Services

Under this model, your IT services company becomes your IT department, supporting all the devices and PCs connected to your server. Managed IT service plans also typically offer phone and on-site support, antivirus, security, backup and a host of other services to monitor and proactively maintain optimal performance and security for your computer network. You'll pay a monthly fee based on the number of servers, computers and devices that need monitoring and support.

Choosing the Best Model

For most small businesses with a server and at least 5 computers, the Managed IT Services approach is by far

Apple's OS X Security Honeymoon Is Over

Unfortunately, bad guys are business people too. Their time is money, and they follow market leaders. By now, Apple's market share of desktop computers is close to 17 percent. OS X, Apple's operating system, is popular with consumers and enterprises, making it a more interesting target for hackers since it has not been "mined" a lot, and Apple users are under the false impression that their platform is "safe and does not even need antivirus".

Well, a report that was released by security company Bit9 shows that more malware has been found this year for OS X than in the last five years combined. The company found 948 unique samples of malware this year compared to 180 between 2010 and last year. The malware is not yet super sophisticated, and is not hard to remove, but the increase is massive and much more than the increase in Windows Malware.

Still, it's early days yet compared with the fire-hose of Windows based malware which is around 400,000 new strains per day at the moment. However, an interesting fact about OS X this year is that many more software vulnerabilities have been disclosed than in past years. A list shows 276 flaws have been found in the last 12 months, which is about four times higher than the average number found annually over the last 15 years.

It looks like more and more researchers are focused on how to bypass OS X security mechanisms or how to get code to execute remotely.

And looking at the mobile side of the house, according to Net Market Share's September figures, iOS claimed 38.6 percent of the global mobile OS market share. The number of iOS devices in the enterprise might actually be higher. According to Good Technology's Q2 Mobility Index Report iOS had 64 percent of worldwide enterprise market share, although this had dropped from 70 percent the previous quarter.

From the perspective of security awareness training, Apple users need to be trained just as much as Windows users. More than half of the Apple malware found this year was aimed at forcing people to view ads, a malware class called adware. And infections were mostly dependent on social engineering end-users, like downloading what employees should "red flag" as dodgy software.
It is loud and clear that effective security awareness training is a must for *all* employees, regardless their computer, Windows or Apple OS X.

Google Plus: What You Need To Know

Is Google Plus a bust? Or is it still a channel to be reckoned with if you don't want to lose touch with your customers?

Google Plus – aka "Google+" – is a social network built by Google. It's been connected to other Google products. It was the birthplace of Hangouts, for instance, now a standalone product.

But things are changing. Google is dismantling Google+ for parts. What will remain may be just a stream, yet it will likely endure due to its die-hard fan base.

So how relevant is Google+ to your business?

The answer is, it depends on your customer base. Are your ideal customers using it? If not, perhaps you can safely ignore it. However, if you already have a following on Google+, or if you are targeting new customers who use it, here are three ways you can leverage it for your business:

Get Found Fast
It's no surprise that Google Search favors Google+ posts. With a little reader engagement, your post can show up on page one in just a few days.

Give to Gain
Content that helps you target prospects with a simple "thank you" to folks who engage can work wonders.

Build Micro-Lists with Circles
Here's a little-known secret: For circles up to 100, Google+ allows you to "Also send e-mail." This can be a great way to build tightly segmented lists.

Depending on your audience, Google+ may still be the best way to connect with your customers.

…..con'td

Comparing Managed IT Services & Break Fix

...the most practical option and it's not hard to understand why. Regular monitoring and maintenance is critical for today's networks. Protecting computer networks against the plethora of cyber crime activities is a full-time job that requires the full-time monitoring and regular installation of Microsoft updates that managed IT service plans provide.

The prevalence of cybercrime doesn't even take into consideration other common network disasters your network faces including employee mistakes, lost devices, hardware failures, fire or natural disasters that can interrupt or even destroy your IT infrastructure and the data it holds.

Finally, managed services is the most cost-effective option. Monitoring and prevention is far less costly than waiting until a disaster strikes to call IT support. As the saying goes, an ounce of prevention is worth a pound of cure.

As well, managed services plans make it a cinch to budget your IT expenses as most companies offer "all you can eat" plans such that all proactive and reactive support on a monthly basis is included for one flat affordable fee.

New Client Special Offer Thru November

10% off the first TWO months of our Essential or Professional Care Managed IT Service Plans when you sign up before November 30th!

Must have 15 or more PCs and at least 1 server to qualify.
Call Joe Stoll today at
416-489-6312 x 205