ISSUE 6-3

BITS & BYTES

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

IN THIS ISSUE

Are You Prepared For Security Threats 1
Shiny New Gadget of the Month 2
Beware Of Advanced Malware 2
IT Issues vs. IT Problems 3
How To Never Forget A Password 3
Is Your Home A Safe Office? 4
How Safe Is Your Email? 4

MARCH 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

Luck Is For Leprechauns—Is Your Business Prepared For Future Security Threats?

If your business hasn't been the target of malicious intruders or cybercriminals, consider yourself lucky. Hackers are a relentless bunch and they want your gold: information and access they can use to exploit loopholes in your business's Internet security. The last few years have been hard on companies all across the globe. And these cyber-breaches aren't going to stop simply because the "damage has been done." In the US and Canada, reported incidents have affected over 215 million consumers and over 7 million small businesses. And that's only counting the attacks that authorities have uncovered.

For cybercriminals, there is no end game. All too often, small business owners assume they are outside the firing line and hackers aren't interested in them. While the media focuses on the big cyber-attacks, there are countless other stories playing out at small businesses everywhere. Cybercriminals are constantly in search of loopholes and weak security. And, unfortunately, small businesses often have the weakest IT security.

Security industry analysts predict that 2015 won't be much different from 2014 when it comes to cyber-security. There are going to be more data breaches. It's just a matter of where and when. It's also a matter of being prepared.

Free Cyber-Security Audit

During the month of March, we are offering our readers a FREE Cyber-Security Audit to help uncover loopholes in your company's online security. At no cost or obligation, one of our highly trained senior IT pros will come to your office and conduct this comprehensive audit. And after we're done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and a Prioritized Plan Of Attack for getting any problems addressed fast.

Because of the intense one-on-one time required to deliver these Cyber-Security Audits, we can only extend this offer to the first seven lucky companies who request it by March 31st. All you have to do is call Joe Stoll at 416-489-6312 x 204.

Shiny Gadget Of The Month:

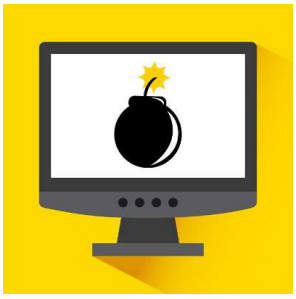
The Withings Activité Pop

Lately, it seems the tech world has been inundated with wearable devices, from fitness trackers to smartwatches. They offer a number of useful features, but they also lack in elegance. They are often bulky, ordinary, complicated and—in the case of smartwatches—have less than desirable battery life.

This is where the Withings Activité Pop comes in. It looks like a classy watch on the outside, but on the inside it's a very different story. It's an activity tracker, verging on expressing itself as a smartwatch.

From the smartphone app, you control everything, from the analog dials to your activity goals. The watch face features a secondary dial that tracks your activity—from 0% to 100%—for the day. It's simple and straightforward. It's water-resistant up to 30 meters and available in three colors: azure, sand and shark gray. It's currently available at Best Buy, in-store and online.

Advanced Malware Is Targeted, Stealthy, Evasive, & Adaptive



The online world is a scary place. Viruses, malware, spyware, adware, and more are all out there trying to get at your network. These threats are almost always prevalent, but compared to each other, some are vastly superior and far more dangerous and advanced than the others. Advanced malware has the potential to disrupt your business's operations, cause extensive data loss, and more.

Processor magazine digs deeper into what makes advanced malware so much more dangerous than the typical malware you encounter most of the time. Robert Clyde, the international vice president of ISACA, explains how advanced malware operates: "The nature of advanced malware is that it's targeted, it's stealthy, it's evasive, and it's adaptive." All of these traits combined turn the traditional malware variety into a lethal, targeted dose of annoyance designed to bring down even the largest targets.

Generic malware is typically created to disrupt a system and wreak general havoc. Unfortunately, advanced malware is far more complex than that. It's usually designed with a specific target or goal in mind. More often than not, the purpose of this advanced malware is to collect information, infect key systems, or sabotage particular data, and it's designed to fulfill this purpose in the most convenient and reliable manner possible. The term, "Advanced Persistent Threats," might come to mind, and it's often used to describe threats which aim to meet their goals over an extended period of time, rather than immediately.

Defenses put into place against standard malware varieties aren't the best way to combat these dangerous strains. It's not uncommon for these threats to cause more trouble as soon as they're identified, and they can spread the contagion throughout your network by jumping from system to system. This makes it far more difficult to corner and eliminate them.

The easiest and most practical way of dealing with these kinds of threats is by taking advantage of Technical Action Group's Unified Threat Management (UTM) solution. This is a four-pronged offensive against malicious entities that can be found online. The first step is to protect your business's network from getting infiltrated in the first place, and that's where a powerful firewall comes into play. This acts like a bouncer, keeping only safe and secure data from accessing your network. It also keeps threats from leaving your network if they've been detected, allowing for a prompt deletion.

Other preventative measures that are taken include integrating a powerful spam blocking solution, as well as a content filtering protocol. This keeps dangerous and persistent spear-phishing threats from targeting you by eliminating the majority of time-wasting and annoying spam, and protects your team from accessing sites which hold potentially malicious code.

And, finally, the UTM integrates an enterprise-level antivirus software into your IT strategy which is capable of detecting and eliminating the nastiest threats on the Internet. This helps you maintain control of your network at all times. If you're not sure about your current network security situation, Technical Action Group provides free network security audits that are liability-free. This lets you confirm your suspicions and take steps to prevent the situation from getting worse.

If you're not sure how to proceed, calling Technical Action Group is the best decision you can make. We'll help you locate and exterminate current threats, and take proactive steps toward securing your network from new ones. Just call Joe Stoll at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com for more information.

Can You Tell The Difference Between An IT Issue And An IT Problem?

We often discuss why it's important that a business takes proactive measures to resolve IT issues before they become problems, but these definitions might be lost on some of our followers. In order to understand the true value of our IT services, it's imperative that you're able to distinguish the difference between these two disruptive sources to your technology.

The hard truth is that it can often be difficult to discern a technology issue from a problem, but if you're in need of a cold, hard definition for the two, we've put these together:

An IT issue is one which is potentially disruptive to everyday operations, but it may not be apparent at the present moment (i.e. it's not immediately effecting your business). An IT problem is basically an IT issue which has matured. It is the result of not dealing with minor disruptions as they happen. It is now negatively affecting your business.

One of the biggest differences between an issue and a problem is that one of them is easily preventable. To help you further understand the difference, we've put together a few scenarios which can be prevented thanks to proactive IT services.

Security Discrepancies

You're checking your email and you see what looks like a perfectly legitimate sign-up form from one of your favorite websites. However, what you didn't realize is that the URL to the form starts a download, which in turn installs malware on your system. In a situation like this, all of your pains could have easily been avoided if that email didn't make it to your inbox in the first place.

In this case, email spam is the technology issue which could lead to malware or viruses infecting your system, which is the problem. TAG's Unified Threat Management (UTM) solution is designed to keep threats out of your system, and quickly neutralize the threats that do land in your network. In this particular case, the UTM provides spam blocking features which prevent suspicious emails from making it to your inbox in the first place.

Putting Off Maintenance

You know your business's technology needs to be up-to-date and current, but in the throes of business it can be difficult to remember when patches and updates should be applied. Not applying the latest patches and updates to your operating system and your software is like leaving a wide-open hole in your defenses, and you're practically begging for a threat to get through.

If you're thinking the issue is the unapplied maintenance, then you're right. Neglecting proper maintenance leads to potential vulnerabilities and security breaches. With a proactive maintenance solution from TAG, your servers, desktops and laptops receive regularly scheduled updates so all your systems are always up to date and secure.

Data Loss

A business that doesn't keep external backups of their data stands to lose it all. Let's say a flood wipes out half of your office. Technology certainly isn't water-proof, so naturally your servers and workstations take some serious damage. In the event a disaster strikes such as fire or theft, your hardware could be destroyed or taken; and with it, your data. Businesses who can't access their data for an extended period of time likely won't be in business for much longer, so it's important to take potential issues such as fire, flood and theft into account.

Never Forget A Password Again With A Password Manager

We all have a number of passwords. You name it: banking, online bill payment, e-mail, social networks, shopping, etc. It's easy to lose track of them all unless you are committing one of the greatest online security offenses by using one password for everything. One of the most secure ways to handle your passwords is with a password manager.

It's not uncommon for password managers to get overlooked when it comes to online security. There is a false concern that keeping all of your passwords in one place can potentially open up all your protected accounts to intruders—if they are able to break into the password manager. It's a legitimate concern, but password managers use powerful encryption to keep your passwords safe. They are specifically designed to keep you even more secure than you otherwise would be.

Many password managers—including LastPass, KeePass and 1Password do more than "remember" your passwords. They also offer password-creation assistance, tell you if a password is too weak or just right. Some managers offer to generate a secure password for you. Since you don't need to remember it, it can be more complex. They are compatible with a number of platforms and packed with customizable tools to keep you safe.

In this case, the issue is a lack of data backup, and the problem is data loss. Data backup is sometimes considered an afterthought for some businesses, even though it should be a top priority. TAG's Backup and Disaster Recovery (BDR) solution prepares your business for any type of data loss disaster, whether it's caused by hardware failures, natural disasters, or hacking. You'll enjoy several backups throughout the day, and a quick recovery time to minimize downtime in the event of disaster.

If you're ready to take the first step toward a proactive IT policy, give Joe Stoll a call at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com. We'll make sure your recurring IT issues don't become even greater IT problems.

How Safe Is Your Email?

Email is (and has been) a prime method of communication for businesses of all sizes. With email comes a whole slew of issues that are essentially synonymous with the technology; spam, information overload, phishing, and information privacy. Even Toronto small businesses that only do business locally are at risk of these issues. Personal email accounts are equally at risk. Employing proper precautions and practices whenever communicating via email is very important to prevent the risk of security compromises, monetary loss, and even legality issues.

Spam Inundation

If you've been using email for a while either professionally or personally you have almost certainly gotten email from people you don't know. Most of these emails are blatantly unwanted while others can look 'almost' legit, as if a real person is trying to contact you. Often (and unfortunately) spammers can get your email address when you put it online or use it to register for accounts on sites on the internet. The good news is standard spam protection is getting better these days, and more advanced spam protection is cost effective for businesses that need the extra layer of protection. Spam can cause a lot of harm for a business network if it isn't kept under control - spam can bog down email servers and eat up network bandwidth and plus it drastically slows down employee productivity because they need to sift through it all just to find their real email. If you and your staff are getting more than a few spam emails a day, contact us at 416-489-6312 x 204 and ask Joe about our anti-spam solutions.

Keep your Computer Safe

Be sure to keep antivirus definitions up to date, and run scans regularly. Running adware and spyware removal software at regular intervals is important too. Be sure your Windows Updates are up to date as well. For businesses, you'll want to invest in network protection to keep external threats from leaking in. Even for small businesses, security and threat management is important to keep operations running smoothly and to prevent expensive downtime and data theft.

Don't Rely on Email for Storage

Everyone has done this at least once; you are working on a report or document on one computer and you email it to yourself in order to pull it up on another computer. That's fine as long as you mind your inbox capacity, but you shouldn't rely on email for storing files, not even as a reliable backup. Imagine having to painstakingly pick through all of your email to restore your most important files. It doesn't sound like a good idea now, does it? On top of that, email isn't any less prone to data corruption or loss than any typical storage solution, and unless the server hosting your email is backed up with a reliable solution, it could be here today and gone the next.

Does Working From Home Threaten Your Business's Data Security?

As a business owner who also spends time working from home, do you make assumptions about your home's wireless network security? It's easy to assume that since your businesses' network is locked down, your data is secure. But when an intruder wants to access your businesses' proprietary information, they're going to search for the easiest point of entry.

Your home tends to be that place. Intruders look for information they can profit from, including financial and identifying data. If your home's wireless is underprotected, you could very easily end up having this information stolen from you—and by the time you notice the damage will have been done.

What Can You Do To Protect Yourself & Your Company Assets?

Be aware of when you're sharing data. If you have any files in a public folder, move them to a more secure location.

Use a strong password for all your wireless networks. A string of letters, numbers, and symbols about 14 characters long is ideal.

Use WPA2 security, and make sure your router is set up correctly. If you are using WEP or WPA security, change it as soon as possible. Change your network's name (SSID). Routers include a default name, and keeping the default tells potential intruders lax security measures may be in place.