

## We've Moved!

We've moved offices! After growing significantly over the past year, we decided it was time to move to larger offices. It was definitely getting cramped in our previous space.

Since communication and collaboration are central to our operations we also wanted a more open-concept space.

Don't worry, this won't affect response time—we only moved 2 blocks!



We're really enjoying our new space, and if you're in the area we'd love to show you around, have a chat and make you a cup of coffee!

We're located right by Dufferin and Lawrence at 75 Dufflaw Road, Suite 201B.

**April 2018**



This monthly publication provided courtesy of Ted Shafran, President of Connectability



## Don't Ever Let Your IT Company Do This To Your Computer Network

Today, when companies need to be lean, nimble and brutally efficient to survive in a competitive marketplace, cutting unnecessary costs is paramount.

Unfortunately, it can be easy when you're on a tight budget to accidentally strip away components of your business that may seem gratuitous but are actually essential to your success.

One of the first things that often ends up on the chopping block in the frenzy to save money is IT. Instead of continually investing in managed IT services, where professionals carefully maintain, protect and update your network month to month, some businesses decide that the best way to keep their technology running smoothly is to simply leave it alone, calling up a professional only when something breaks down.

Of course, this approach forgoes monthly costs and shaves off a fair few dollars from

your technology budget in the short term. But while this approach may seem cost-effective, it opens up your business to a huge variety of technological crises, from expensive network outages to cyber-attacks that may cripple the very future of your company.

### The Problem With A 'Break-Fix' Strategy

It can be hard to imagine the huge list of problems that might arise within your network. So, it's an understandable strategy to wait to do something until an issue becomes a serious problem. At that point, they bring in a professional who - charging by the hour - attempts to find and repair whatever may be broken.

It seems like a logical approach, but unfortunately, it's littered with huge hidden costs. If you're calling an IT expert only when

*Continued on pg.2*

*Continued from pg.1*

something in your network is broken, only your most urgent technological needs are addressed. When your technician is being paid an hourly wage to fix a specific issue, there's no incentive to be proactive with your system. They won't recommend important, money-saving upgrades or updates, and they will rarely be able to detect a crisis before it happens.

What's more, the "if it ain't broke, don't fix it" approach very likely leaves huge holes in your security and drastically magnifies the costs of an IT meltdown. If they're only arriving in the midst of crisis, there's hardly ever an opportunity for the break-fix technician to strengthen the barriers between you and the hordes of hackers clamoring for your data. They're on the clock, being closely monitored to fix the problem and then go away. Meanwhile, the security landscape is constantly changing, with criminals and security experts in a back-and-forth arms race to

**"Instead of continually investing in managed IT services...business owners decide that the best way to keep their technology running smoothly is to simply leave it alone, calling up a professional only when something breaks down."**



stay abreast of the latest developments. Without someone managing your system on a regular basis, your protective measures are sure to become woefully out of date and essentially useless against attack.

### Why Managed IT Services Are The Answer

When you turn over your IT needs to a managed services provider (MSP), you're entrusting the care of your network to a team of experts who have a real interest in your success. MSP engineers regularly monitor the health of your system, proactively preventing disaster before it enters into the equation and hurts your bottom line.

Beyond this preventative care, MSPs do everything they possibly can to maximize the power and efficiency of your equipment, implementing only the best practices and the latest software and updates.

When you invest in an MSP, you may have to invest more funds initially, but likely you'll save tens of thousands of dollars in the long run by avoiding cyber-attacks, downtime and hourly rates wasted on a technician who doesn't really care about the future of your business. When you choose an MSP, you're not just choosing a superior and healthier network - you're choosing peace of mind.

## Free Report: What Every Business Owner Must Know About Protecting And Preserving Their Network

### PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"



Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report outlines in plain, nontechnical English common mistakes that many business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your **FREE** copy today at  
[www.connectability.com/protect](http://www.connectability.com/protect)  
 or call our office at (416) 966-3306

## Shiny New Gadget Of The Month:



### 4K HDR Projector Can Beam A 150-Inch Picture Onto Your Wall

A 65-inch OLED TV is a beautiful thing. But can it compare to a crisp, bright 150-inch display in the comfort of your home?

That's what LG is offering this year with its new 4K HDR projector, the HU80KA. Clocking in with a 3840 x 2160 resolution, 2,500 lumens and a stunning picture, the portable device is an attractive offer indeed.

The device is only a few feet tall, but it looks like it will be the ideal piece of equipment for home theater enthusiasts. It's the closest you can get to the big-screen experience, and you won't even have to plunk down 20 bucks for a tub of popcorn. It remains to be seen, though, whether it'll be worth the price tag. At the time of writing, the price has not yet been released, but bulkier, less portable competitors cost a little under \$2,000.

## Story Time

Welcome to the inaugural edition of *Story Time*, a collection of stories and experiences we've amassed over our 23 years in the IT business. Most stories focus on a single theme related to customer service, IT support, network security, administration, or even just tips and tricks we think more businesses should adopt.

This month I want to focus on cybersecurity since we've had some situations recently that highlight why it's so dangerous to assume your network and the data it contains is secure.

I want to share a couple of cautionary tales that may scare you, but should encourage you to take a hard look at your cybersecurity:

One company experienced a Ransomware attack that left their entire office at a standstill. The price to get their data back was over \$30,000! Worse still, it took days to get the decryption key after they paid the ransom. Unfortunately, we were brought in only after all this happened. With the preventative measures we've put in place, there's very little chance of this happening again. But if those protections had been in place earlier, the company could have saved a considerable amount of cash, plus the hidden costs associated with downtime.

In our second story an employee received an email from the CEO—who was out of the office—requesting a large wire transfer to a foreign bank. Fortunately, the employee had the common sense to pick up the phone and call his CEO. If he had sent an email instead, he would have received an approval—but from the hacker. Someone had managed to get one or more passwords for the company's email accounts and was attempting to use them to commit fraud.

Neither of these businesses did anything wrong, in fact, one of them had all the latest security patches and updates, top notch antivirus protection, and a business-grade firewall. But unfortunately, that's not enough anymore. Today, the **#1 way** hackers gain access to your passwords and your network

is **poisoned email**.



It starts like this: a hacker sends you an email pretending to be Rogers, or Microsoft and requests some information. The email seems legitimate and looks just like the emails you normally receive, so you don't think twice about it. You follow a link in the email to a website where you are prompted to enter some information, or you simply reply to their email. At this point a hacker has the keys to your kingdom.

So how can you prevent this from happening to your business? Here are three things you'll need:

- 1) **ADVANCED** mail filtering
- 2) Credential monitoring
- 3) Regular education

Advanced mail filtering reduces the risk of poisoned emails getting to you in the first place. Regular user education reduces the risk of an employee responding to a malicious email if it *does* get through the filter. Finally, if an email gets through the mail filter **AND** someone still opens the link or responds with confidential information, credential monitoring will let you know **INSTANTLY** so you can change passwords and reduce the impact of a breach.

We believe this three pronged approach is the **ONLY** way to completely protect your business from cybercrime, and data breaches. While you need to have perfect defenses, a hacker only needs a tiny hole to make your life miserable.

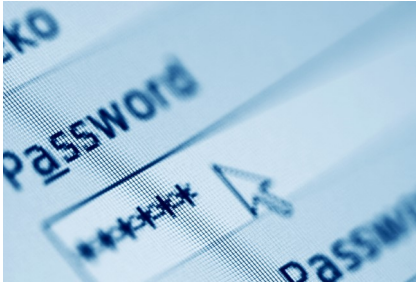
If you're interested, give us a call at 416-966-3306 or email us at [info@connectability.com](mailto:info@connectability.com) and we can show you how you can prevent a data breach from wreaking havoc on your business.



### ■ Here's The Reason You Need So Many Different Passwords...

Thinking up passwords and managing them is a big pain, no doubt about it. One website requires a symbol, and another requires 14 characters. Meanwhile, your bank requires 10 characters, four PIN numbers and the answer to a secret question. In the midst of all this, it's easy to just use the same three or four passwords for everything — after all, that's more secure than a single password, right?

But imagine this. Say you use the same password for your Gmail, your Amazon and the account you



use to order gift cards at a 10% discount for client gifts. One day, the gift card website is hacked. Not only do the crooks get your credit card info, they also get the list of all the website's users and those users' passwords. Then, they publish these freely on the internet.

But if you use different passwords for all your accounts, you're safe despite any crisis that may arise. Make sure you practice good password security.

### ■ 4 Ways To Improve Customer Satisfaction And Increase Your Profitability At The Same Time

**1. Host an event.** In B2B companies and small businesses that have a highly specific and local customer base, a big appreciation event can go a long way. Just make sure to view attendees as friends rather than customers you're trying to close on.

**2. Personalize your services.** If you're able to tailor your offerings to your customers' desires, that extra effort can really impress the people you serve. It doesn't have to be complicated. Get creative and add that little bit of human touch to your product.

**3. Send handwritten notes.** E-mails, social media and phone calls are great, but if you want a thank-you card or customer appreciation note to stand out, it's best to write them by hand.

**4. Launch a loyalty program.** These programs can increase profits for you and your business, but they'll also have the benefit of making your most loyal customers feel engaged and appreciated.

*SmallBizTrends.com Jan. 16, 2018*

## Tales From The Trenches

Do you ever feel like no one listens any more?

We sure do. We moved our offices on February 20 of this year. And back in December, we called our alarm company - one of the biggest in Canada - to let them know. They told us it was much too early, and that we should call back in late January.

When we called them back, they assured us that they would have an installer in our new offices on moving day. But when they arrived, it turns out that they had sent a **salesman**. He was totally confused and when

he called his company back, they agreed that they had made a mistake but still said it would take 5-7 days before they could arrange an installation.

Needless to say, we went with another company. Not only did they install the alarm right away, they were actually less expensive.

At Connectability, we always aim to practice **Active Listening** so that we understand your problems and your needs, and respond appropriately. We think that's a courtesy all businesses need to extend.



This month we'll be donating to The Salvation Army. As I'm sure many of you already know The Salvation Army is an organization that focuses on giving hope and support to vulnerable people in 400 communities across Canada and in 128 countries worldwide. We wanted to contribute because of their dedication to fighting homelessness, something all too prevalent in Toronto.

If you're interested in contributing we'd love to hear from you. Email [info@connectability.com](mailto:info@connectability.com) or call our offices at **(416) 966-3306**