Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Beware The Big Box!

If you buy cables, toner, ink, or other accessories at big box stores **STOP RIGHT NOW!**

Those stores charge an arm and a leg for accessories, so you could be paying $30 for a cable that costs $5 elsewhere.

Your best bet: buy them on Amazon, or through a site like Monoprice.

Alternatively we sell peripheral equipment at significantly lower prices than Big Box stores.

And if you're looking to buy computers, switches, servers, etc. we can help there too. Our prices are reasonable and we have the expertise to find the best possible solution for your business.

May 2018

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

The Shocking Truth Behind Cybercrime Threats

And What You Can Do About Them Now

Today's technological innovations have empowered small businesses to do things that would have been utterly unimaginable even 15 years ago. To remain competitive in a constantly shifting landscape, we've become more dependent on software and hardware to house even the most basic structures of the companies we run.

Meanwhile, these technologies are evolving at breakneck speed. Every day, there's a slew of new devices to consider, a pile of new updates to install and a new feature to wrap our heads around. Every morning, we wake up and the digital world is thrillingly new.

But all over the world, there's an insidious network of criminals keeping up with this insanely rapid pace of progress. With every new security measure designed to protect our digital assets, there are thousands of hackers working around the clock to determine a new way to break through. An estimated 978,000 fresh new malware threats are released into the world each day. The term "up to date" doesn't mean much anymore in the wake of new developments arriving minute by minute.

There's a price to pay for the increased efficiency and reach enabled by the digital age. We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a crippling large-scale cyberattack, with criminals lifting millions of dollars in customer data and digital assets. Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and Target – these narratives are so commonplace

Continued on pg.2

Continued from pg.1

that they barely raise an eyebrow when we read about them in the news.

Most business owners wrongly assume that these incidents have no bearing on their own companies, but these high-profile incidents account for less than half of data breaches. In fact, according to Verizon's 2017 Data Breach Investigations Report, 61% of attacks are directed at small businesses, with half of the 28 million small and medium-sized businesses (SMBs) in America coming under fire within the last year.

It's hard to imagine how you can possibly protect yourself from these innumerable threats. Statistically, you can be all but certain that hackers will come for your data, and there's no way to know what new tool they'll be equipped with when they do.

You may not be able to foresee the future, but you can certainly prepare for it. With research, education and resources, you can implement a robust security solution into the fabric of your business. That way, you can send hackers packing before they get their hooks into the organization you've spent years building from the ground up.

> **"We've all heard the story before. A massive, multinational corporation neglects some aspect of their security and falls victim to a large-scale, crippling cyber-attack..."**

One huge leap you can make right now for the security of your business is to simply realize that cyber security isn't something you can install and leave alone for years, months or even days. It requires regular updates and the attention of professionals to ensure there's no gap in your protection. There are new shady tactics being used by criminals every day, but there are also fresh protocols you can use to stave them off.

Small business owners assume that since they don't have the resources of a Fortune 500 company, they don't have the means to invest in anything but the barest of security. Obviously, hackers know this and target SMBs in droves. The bad news is that most businesses' paper-thin barriers won't save them in the event of a crisis. The good news is that it doesn't take thousands upon thousands of dollars to implement a security system that will send the hackers packing.

Are Mobile Devices Putting Your Business At Risk?

There's no question: mobile devices have made our lives a lot easier. You can get directions, check your email, purchase basically anything, and check on your laundry - from anywhere in the world with the touch of a button. Unfortunately, with all these benefits comes added complexity and a lot of risk.

When smartphones hit the market in the early 2000's their were no viruses or security threats. Unfortunately those days are long gone. More and more, viruses and malware are being crafted specifically for mobile devices. So what happens if a device with company data is hacked? Or what if your device is lost or stolen? How does your response change if the device is owned by an employee vs. company owned? That's where **Mobile Device Management** (MDM) comes into play.

MDM supports iOS, Android, Blackberry and Windows devices and is primarily used for creating policies and enforcing compliance. MDM can be used to: restrict device features and application downloads, enforce device encryption and password policies, and much more.

If you want to learn more about MDM and how it can reduce the risks of mobile devices for your business call us at (416) 966-3306

Shiny New Gadget Of The Month:

This Reverse Microwave Can Quick-Freeze Food And Drinks

Way back in 1946, technology gave us the ability to pop some leftovers into the microwave and heat them up within minutes. But if we had a warm beer in our hands or needed a tray of ice quick, we were out of luck. Enter Frigondas's line of new kitchen technologies, which enable users to flash-freeze dishes, rapidly chill beverages and create crystal-clear ice within minutes. Couple this revolutionary feature with Frigondas's host of advanced heating abilities, and you've got a kitchen appliance that's set to change the microwave game for good.

The only problem is that the technology isn't yet available for purchase, with no release date in sight. Still, experts expect it to hit the market within a year or two, though it remains to be seen whether it will justify what's sure to be a hefty price tag.

Ransomware On The Rise

There's no doubt about it, the threat of **Ransomware** grows every day. A Ransomware attack is when a hacker encrypts your computers and all of your data until you pay them to decrypt it. They generally charge between $5000 and $50000, but it can be more for large organizations. If this sounds scary that's because it is.

Every year Verizon releases a "Data Breach Investigations Report" outlining the most major security threats every year. In 2014, Ransomware was the 22nd most common malware type. In 2017 it ranked 5th, and this year it ranks #1.

The data was collected from 67 organizations in 65 countries. There were 53,000 incidents and more than 2,200 breaches over 2017. Today 39% of all data breaches involving malware are Ransomware incidents. That's **DOUBLE** the proportion from 2016. Another report released by the CEO of Malwarebytes said "2017 was the year of Ransomware, especially in B2B" and things are only getting worse.

So why the rapid increase? Hackers only need one hole in your systems and - boom - they can lock you out completely. Until you pay the ransom, your business is on hold. Therefore many businesses pay - and quickly.

Phishing is the most common method hackers use to gain access to company networks, but pretexting is growing. With phishing a hacker sends a legitimate looking email. The intent is to get you to open a link that installs harmful malware. Pretexting is a bit different. It is a type of social engineering. A criminal pretends they need info from you to confirm your identity. After establishing trust they'll ask some "innocent" questions designed to gather information that will help them gain access to your systems. They don't need you to download anything, they just need a little trust.

Why Ransomware? As you might expect, a majority of attacks are financially motivated, although there are situations where a hacker is hired to gather private company data.

So how can you protect yourself?

It's simple! We offer a solution called **SentinelOne** that was originally developed for large enterprise customers. It is an advanced security solution capable of stopping even the newest, most sinister threats.

SentinelOne uses machine learning and AI to continuously stop threats that don't yet exist so you can work, live and use technology without worrying about threats or being encumbered by intrusive security.

If they aren't able to keep you safe from a Ransomware attack they'll reimburse you $1000 USD per affected endpoint, up to $1,000,000. That's how committed they are to making sure your business is protected.

For just **$7.50 per computer** per month you get the peace of mind of knowing that you have the very best protection on the market. If you'd like to learn more about SentinelOne and how it can help secure your business give us a call at **(416) 966-3306** or email us at **info@connectability.com**

Your Bank Account Is Vulnerable

Imagine this: you get to the office on Monday morning feeling a bit groggy. You grab a coffee and sit down at your desk when you realize you need to pay a few bills. No problem. You open up your browser, navigate to your banking portal, make a few transfers, and voila, all done. BUT what you don't know is that there is **malware** on your computer monitoring your activity, and storing your account passwords. Uh oh. Even worse, you probably won't know until you find out that your bank account has been completely drained.

Luckily there is a simple solution: use a dedicated Chromebook for your online banking!

Chromebooks offer some security features that can't be matched by Microsoft or Apple operating systems:

1) **Sandboxing:** each program running on your computer is completely isolated from one another. That way if you encounter malware while on the internet it won't infect the rest of your machine.
2) **Automatic updates:** Chromebooks are split into two partitions—the one you are currently using, and a background copy. Whenever an update is available it loads in the background, and the next time you start up your machines (takes 6-10 seconds) you are running the most up-to-date operating system. You'll never have to sit around waiting for updates to finish again!

For an investment of $200-$300 we believe a Chromebook is the best way to **SIGNIFICANTLY** reduce your chances of a financial breach. If you want to learn more, or would like us to order you a Chromebook, email us at **info@connectability.com** or call **(416) 966-3306**

3 Big Trends Businesses Need To Adopt Now

When the online publication Small Business Trends surveyed nearly 500 small and midsize-business owners across the country last February, they found that technology has become more important than ever in companies of all sizes.

Though CRM is often an expensive and lofty goal for time-strapped businesses, it drastically increases growth once it's implemented and understood. In fact, Small Business Trends found that "growing SMBs are twice as likely as their stagnant counterparts to rely on CRM in their daily lives." Along with these cohesive programs, synchronizing business data across platforms is becoming a priority as well, especially when providing a holistic view of key customer information.

Even artificial intelligence has begun to crop up in the small business market, albeit slowly. Still, it's clear that the fastest-growing businesses are using automation and predictive sale forecasting nearly twice as much as their stagnant counterparts.

SmallBusinessTrends.com, 2/14/18

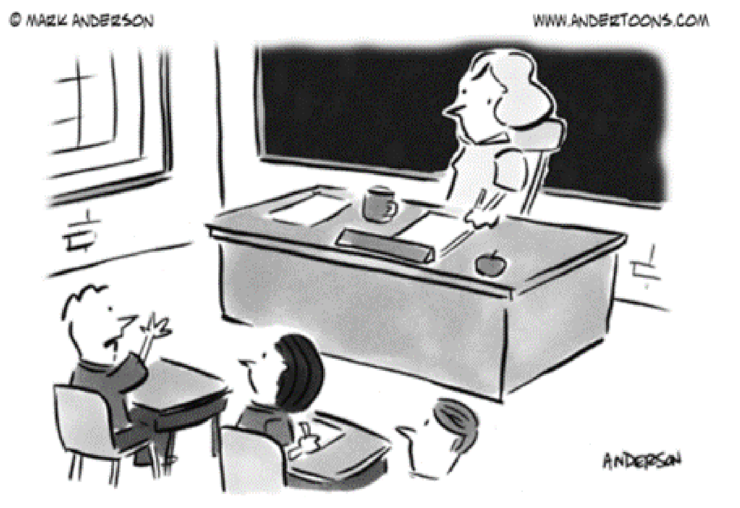
The Internet Of Things: Are You Okay Playing Offense?

Adjusting your home's thermostat and hot water heater back to normal temperatures as you board a plane on your way home isn't just cool, it's incredibly handy. However, the network of these and other connected devices – called "the Internet of Things" (IoT) – poses one of the biggest security problems of the modern era.

Most people think about changing their computer password regularly and their ATM PIN occasionally, but they almost never consider changing the password the programmable thermostat ships with from the factory, meaning that anyone who can access the manual has access to your thermostat.

Usually, attackers who target IoT devices don't want to cause you a problem. Instead, they use your device along with 20,000 other thermostats as "soldiers" to battle against a website or e-mail server. By flooding these sites with traffic, they can shut them down or stop your e-mail server from delivering your messages.

You should adopt a strict offensive posture against these types of threats in your life and business. If there is even a suspected problem with one of your IoT devices, pull the plug. Your heater may be cold when you get home, but at least your data will be safe.



"How come Lewis and Clark didn't just use MapQuest?"

This month we'll be donating to **360°Kids**. They began their mission 28 years ago as two separate organizations: The Markham Neighbourhood Support Centre and Youth Housing Markham. They eventually became 360°Kids.

360° kids
Surrounding kids in crisis with care

This name refers to the comprehensive approach they take in assisting at-risk youth and surrounding them with care, recognizing that these kids need a wide range of support to help them rebuild their lives. They now serve over 3000 youth across the GTA each year.

Their slogan? "Surrounding kids in crisis with care"

As always, if you'd like to help we'd love to hear from you. Email **info@connectability.com** or call us at **(416) 966-3306**