

## The Internet of Things (IoT)

20 years ago a smart home was an extravagant, far fetched idea, but today it's more accessible than ever.

With a Wi-Fi connection, a smartphone, and a few accessories you can transform your home or business into a lean mean smart machine!

You can turn lights on and off, lock and unlock doors, set alarms, monitor your home, start your laundry, and cook a roast all from your smartphone.

Unfortunately, the more devices you connect to the internet the more entry points there are for hackers and cybercriminals.

To protect your Internet-connected devices check out our **"Gadget of the Month"**

**February 2018**



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



## WARNING: Your Business Is More Likely To Be The Victim Of Cybercrime NOW Than Ever Before...Take These Steps Today So You Don't Get Hacked!

Though we're in the midst of an unprecedented rise in high-profile cybercrime incidents, it's easy to assume that our own much smaller businesses are safe. Sure, we think, hacking into the data stores of J.P. Morgan, the U.S. Government, or Virgin America can net hackers millions or even billions of dollars. Why would they bother with a small business?

But unfortunately for all of us, hackers *do* bother with small businesses across the country – these attacks just don't make the news. By some estimates, including one reported in Media Planet, more than half of small businesses have had data compromised. According to StaySafeOnline.org, attacks targeting small to midsize companies now comprise over 70% of all data breaches. What's worse, this digital onslaught shows no sign of slowing. In fact,

ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime.

Once you see the numbers, it's easy to understand why hackers seek the little guy. These days, massive corporations like Google or Citigroup employ incredibly sophisticated digital measures. Their digital vaults, though they contain ludicrously attractive sums of money, are located at the end of a virtual labyrinth covered in traps, with a final, inches-thick steel door protecting their assets for good measure. In contrast, the digital assets of small businesses are often hidden behind nothing more than a single, often weak, password. With thousands of business owners going about their day-to-day, oblivious to their paper-thin security, the question turns from "Why would

*Continued on pg.2*

*Continued from pg.1*

hackers bother with my small business?" to "Why *wouldn't* they?"

Though cybercriminals may come away with less than they might have had they targeted a Fortune 500 company, it certainly isn't going to seem cheap to you. According to one TechRepublic analysis, an average cyber-attack on a small business can cost as much as \$256,000. Is that a sudden expense your company can weather?

Luckily, there is hope. Though small business owners often assume that effective cyber security solutions lie far outside their budget range, robust digital security is more affordable now than ever. By investing in comprehensive protection, small businesses can deflect even the most persistent hackers.

Today, a cyber-attack on your business is almost statistically inevitable. And when that attack comes, you'll definitely want to be prepared. If you haven't needed a doctor for the past two years, does that mean you're going to abandon your health insurance coverage? Of course not. What about car insurance? Does it become unnecessary in the absence of a crash? No, because even if you're the best driver in the

**"What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime."**

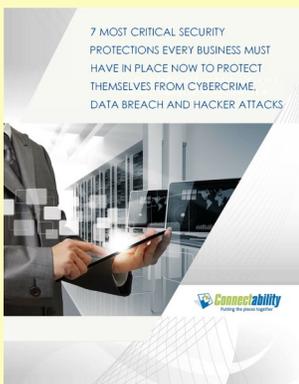


world, sometimes a collision is out of your control.

What's more, both your body and your car require regular upkeep and maintenance to remain in peak condition. It's no different with network security. As technology advances at an incredible rate, the ways that hackers can infiltrate your network multiply. The best security platforms constantly update, enabling them to anticipate these shifts and prevent them from becoming liabilities. This way, you can be proactive prior to a digital crisis, ensuring that no matter what comes, your network is protected.

Even as digital crime climbs at a staggering rate, and hundreds of small businesses are forced to close their doors for good, thousands of owners fail to notice, assuming they'll somehow be spared from an attack. Don't just hope. Invest in regularly maintained, powerful cyber security, and ensure the future of your company.

## **FREE Report: The 7 Most Critical IT Security Protections Every Business Must Have In Place NOW To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks**



82,000 NEW malware threats are released every day (at a minimum), and businesses (and their bank accounts) are the No. 1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious reputational damage, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you **MUST** read this report and act on the information we're providing.

**Claim Your FREE Copy Today at [www.connectability.com/7protections](http://www.connectability.com/7protections)**

## Shiny New Security Gadget Of The Month:



### Bitdefender BOX 2

If you have a smart dishwasher, laundry machine, oven, fridge, or any smart lights or smart locks, this device is just for you.

These Internet-connected devices undoubtedly make your life easier, but they also raise a number of security concerns. The more you have connected to the internet, the more points of vulnerability your network contains.

That's where the Bitdefender BOX 2 shines!

It provides cybersecurity protection for all Internet-connected devices at home or on the go, management for all of the devices in your home network from one mobile app, and parental controls to monitor your kids' online activities and manage screen time.

The BOX can also help improve your internet speed.

Right now the device is on sale for \$199.99 and includes a one year security license.

## Your Business NEEDS A Disaster Recovery Plan!

"Oh the weather outside is frightful"

This famous lyric certainly rings true this year. With some of the coldest temperatures in decades, pipes are freezing, heating systems are failing, and power outages are widespread.

These issues can cause some disruptions to your day-to-day life, but the effect on your business could be catastrophic. If you experience any of the above you'll have to deal with costly downtime, hardware failures or even data loss.

You can't always prevent a pipe from bursting, or a power outage from happening, but there are ways to reduce their effect on your business.

We all know downtime can cost your business thousands of dollars, yet many businesses have no corporate disaster recovery plan.

At Connectability, we believe EVERY business NEEDS a DR plan to reduce downtime, frustration, and keep your business running smoothly.

As the old adage says: "Hope for the best, but prepare for the worst".

Here are a couple of simple things you can do to prepare for an emergency:



- 1) Buy a **UPS (Uninterruptible power supply)** for ALL servers and any critical machines. With a UPS you'll be able to save your work and power machines down naturally, thereby preventing hardware failures and data loss in the event of an outage.
- 2) Consider a **Business Continuity** device. If a server fails you can start up the device in under a minute, and if you lose power at your office you can start it just as quickly from the cloud via a mobile connection.

If you don't have a Disaster Recovery plan, call us at **416-966-3306** NOW. We'll sit down with you, and help you create a plan to reduce the impact of disasters, remove any holes in your protection, make sure everyone in your company knows what their role is, and prepare a formal DR plan.

Like insurance, you hope you never need this, but if you do, you'll be happy you have it!



This month Connectability will be donating a portion of profits to **Pancreatic Cancer Canada**. Phil Nascimento chose this charity because his beloved uncle passed away from pancreatic cancer about two years ago. Pancreatic cancer is difficult to diagnose and nearly impossible to cure. And research is underfunded, so we felt it was important to contribute. The Foundation's mission is to save lives, by attacking pancreatic cancer on all fronts: research, awareness, community activation and advocacy.

As always if you're interested in contributing to our donation we'd really like to hear from you. You can email us at [info@connectability.com](mailto:info@connectability.com) or call us at **416-966-3306**.



■ **Drop These 4 Habits For A Successful 2018** Today, the business world is more rapid, complex, and volatile than ever before, a trend that shows no signs of slowing down. With that in mind, it's vital that entrepreneurs tighten up their business practices now, not later.

Here are four bad habits to kick in order to shed your company's sluggishness and step fully into the modern marketplace:

1. Procrastinating training investment: Investing in comprehensive training resources, which expands the skills of both you and your employees, can



ensure you stay competitive in the midst of constant change.

2. Amassing knowledge without applying it: With millions of well-meaning advice articles plastered across the Internet, it's easier than ever to learn new principles. But you can't stop there. Actively implement the knowledge you gain, instead of keeping it locked away in your mind.

3. Expecting ideas to come from the top down: Today's savvy business owner doesn't solely channel those at the top of the organization chart. Instead, they welcome ideas from all levels of the company.

4. Busywork: Too many leaders get caught up in output metrics instead of outcomes. Get the numbers out of the way and watch your employees shine. *Inc.com* 11/16/2017

■ **How To Spot A Phishing E-mail BEFORE It Can Do Any Damage** Phishing e-mails are bogus messages carefully designed to look like a legitimate message (or attached file) from a site or person you trust. Their goal is getting you to willingly give up your login info or unknowingly click a link to install a virus. The best of these e-mails look uncannily similar to their real-world counterparts, but there are ways to discern a phishing attempt from a legitimate e-mail.

First, hover over — but don't click on — the URL in the e-mail to see the actual website you'll be directed to. If there's a mismatched or suspicious URL, delete the e-mail immediately. Other telltale signs are poor grammar or spelling errors. And if the e-mail asks you to verify or validate your login or personal information, get out of there.

## A Cheaper Solution for Mobility

Depending on how you and your employees use your computers, a **Chromebook** may be the perfect solution for your mobile workers.

A **Chromebook** is a laptop of a different breed. Instead of Windows 10 or macOS they run Google's Chrome OS. This makes them faster, more reliable and **much cheaper** than traditional laptops.

If you're worried about losing compatibility, don't be. You can check your email and calendars and edit documents in your Google Drive. You can even use Microsoft Office, Photoshop, and almost any Android application.

If your computers are getting a bit long in the tooth, give us a call and we can see if a Chromebook is right for you!



*As always, Dilbert can be relied upon to make light of the winter blues!*

