

TECHNOLOGY UPDATE

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

WHAT'S NEW

WELCOME OUR NEW EMPLOYEE:

Brittnee Orsini
Marketing and Office
Assistant

See Page 7

SEPTEMBER 2017



"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 finally and forever!"

Bryan Lachapelle, B4 Networks Inc.

B4 Networks Inc.
170 Hwy 20 W, Unit 3a, Box 249
Fonthill, Ontario, L0S 1E0
Tel: (905) 346-4966

What Will You Do When This Disaster Hits Your Business?

In today's world of rampant cybercrime, every savvy business owner knows the necessity of locking down their data.

However, we find that the cyber security technologies used by the vast majority of businesses are woefully out of date. Sure, your current solution may have worked great, but digital threats to the safety of your company are constantly evolving. Criminals will eventually attempt to breach your data — and your barriers are not as secure as you might think.

Before World War II, the Germans developed a technology that would prove to be a key player in the conflict: its family of infamous Enigma machines. These devices, about the size of a small microwave, were composed primarily of a typewriter and a series of three or four rotors. By using a set of rules contained in a corresponding codebook, German soldiers would use the machine to encode vital messages to be sent covertly over the airwaves. The number of potential permutations — and thus solutions — for the code was in the tens of millions. The Germans were confident that the code could never be broken and used it for a vast array of top-secret communications.

The code's impenetrability didn't last. Via photographs of stolen Enigma operating manuals, the Polish Cipher Bureau reconstructed one of the stubborn Enigma machines, internal wiring and all, enabling them to decrypt the Wehrmacht's messages from 1933 to 1938.



What Will You Do When This Disaster Hits Your Business? (Continued)

Facing an impending German invasion, Poland decided to share these secrets with the British. But, at the outbreak of the war, the Germans increased the security of the Enigma initiative by changing the cipher system daily. In response, a British code-breaking team, led by genius English computer scientist Alan Turing, constructed primitive computers, known as "bombe," that allowed them to decrypt the incredibly complicated ciphers faster than ever before. But it wasn't until the capture of the U-110 warship and the seizure of its Enigma machine and codebooks that the British were able to decrypt the most complicated cipher of the war, the Kriegsmarine Enigma. The information gleaned from these decrypts are believed to have shortened the war by more than two years, saving over 14 million lives. Just like you, the Germans believed the systems they had put in place to defend their secrets were impenetrable.

And it's true: the system had few cryptographic weaknesses. However, there were flaws in German procedure, mistakes made by Enigma operators, and failures to introduce changes into the Enigma formula — along with the Allied capture of key equipment and intelligence — that ultimately allowed the Allies to crack the code once and for all.

Take this as a cautionary tale: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures. Though they may not be led by Alan Turing and his crack team, you can bet criminals are constantly chipping away at the defenses of even the most powerful firewalls. The arms race between cyber security companies and cybercriminals rages on behind the scenes, and you can bet that they've already cracked your business's "Enigma." Just look at the massive European cyber attack this past June, which infected computers from over 27 companies across the continent, including those of the largest oil company in Russia, with ransomware. The unimaginable cost of that attack is something you certainly don't want your business to shoulder.

As technology evolves, so does crime. New threats arise each and every day. While solutions are available (and needed), they are notably absent in older software developed at a time before these constantly morphing attacks even existed. Once the enemy has found a way to pick your lock, you need a new lock. Luckily, you have your trusty IT provider, constantly on the lookout for cutting-edge solutions that protect our clients from even the nastiest malware.

For more information contact us right away at (905) 346-4966 or info@b4networks.ca

Here is what a client is saying about us:

"Threats such as business interruption, cyber hacking, and disaster are obviously worse case scenarios when it comes to running a business. Most businesses likely don't think that they will ever be faced with these challenges – and they probably won't. That absolutely does not mean that they should be ignored.

"Developing a DRP with B4 Networks has given me a peace of mind that has allowed me to focus on the important aspects of running the business."

These are very important considerations for our business, however, on the list of priorities, they often fall to the bottom of the list in terms of time and resource allocation. I don't want to have to think about them day-to-day. In developing a DRP with B4 Networks, it forces me to be proactive and put measures in place (once) so that should an emergency take place, I'm just flipping a switch and putting a plan in motion. I consider this an invaluable "insurance policy". This peace of mind allows me to focus on the more important aspects of running the business."



Jordan Sherlock, General Manager
North American Traffic



How serious is Your Company about Securing its Data?

This article will discuss data security at most companies. It will look at some of the biggest mistakes company makes when securing data and some possible solutions.

Today we use technology in almost every aspect of our lives. While that can be a good thing, there is a negative side to it. Anyone with the right technical know how can gain access to your company's data, which they can use to destroy your business empire.

No matter the size of your company, you will need to create a plan that ensures all the data generated is secure. This plan is known as a security program. The program provides the framework that helps to keep the whole organization safe. Some of the Biggest Mistakes that You Can Make in Securing Data:

- Lack of a System on Where to Store Important Data.** When a system is not in place on where sensitive data should be stored, it increases the chances of it ending up in an unsecured location. One way to solve this is if a company creates a policy that categorizes what type of data is considered sensitive.

- Cloud Misuse.** When a company stores data on the cloud, they are essentially storing their data on a hired computer. That means they have no control over it. If the data is of a sensitive nature, then it needs to be encrypted before being placed on the cloud. It is also important to understand the policy of the cloud services provider. It is especially so if you are required to share encryption keys with them.

- Failure to Protect from Internal Threats.** One of the best examples of this kind of leak was the "Snowden" leak. The issue of the leak was because of weak governance issues. For instance, in this leak, the person managed to copy many gigabytes of data without any hindrance. Organizations need to be careful about giving employees access to data when they do not need it.

To fight off any chances of internal leaks, an organization needs to address the insider threats with appropriate controls. The controls need to be able to identify the damage and tell how much data has been stolen.

- Trusting Technology.** One of the biggest mistakes a company can make is to have faith in its technology. It is important to note that as you work to improve security, hackers are also working. They are designing new and creative ways on how to get past your security. It is thus important that you have experts who conduct regular tests on your system. That way, they can help identify any potential leaks before they occur.

- Failing to Invest Enough in Data Security.** When a business faces a data security challenge, it will most times look for a one size fits all solution. In such a case, the company may end spending too little to protect the data effectively. However, a business has to be willing to go further than this. It has to look for the most secure means of keeping its data secure.

- Failure to Protect Physical Devices.** One of the easiest ways to hack a network is by using a device that is already accepted into the system. However, some organizations do not have measures in place to deal with the loss of physical devices. A good organization should have a mechanism that ensures stolen devices can no longer be allowed to access the system.

- Failing to Take Care of the Human Factor.** An organization will spend a lot of money implementing the most complex security measures. However, most organizations drop the ball when handling the human factor. The staff is not well-trained on how to stay secure. There needs to be a training program for both new and existing employees. As changes are made to the security program, employees need to receive additional training.

- Some of the most important Tips to Stay Secure.** If these measures are not being implemented at your organization, you need to start implementing them if you want to stay safe.

- 1. Make Use of Strong Passwords.** One of the easiest ways of keeping your organization secure is by implementing a strong password. Ensure that everyone who has access to your network makes use of a strong password. Use a combination of all character types on your keyboard for the best password. You should also ensure that your password is at least 8 characters long.

Never use any personal data as your password. Additionally, avoid using variations of personal data to create your password. Besides that, ensure that you change your password after every 90 days. It is also important everyone to have his or her own password and username. Having a generic password for everyone is dangerous.

- 2. Make Regular Software Updates.** Another simple but effective measure to keep your data safe is to keep all programs updated often. There is little use in installing the latest software if you will not make regular updates to it. Data is only as safe as the most recent updates to the system.

- 3. Encrypt Portable Devices.** Portable devices such as laptops are quite easy to steal. It is thus important that you take the extra step to ensure they are safe, even when stolen. One of the easiest measures to keep them safe is to encrypt them. The encryption software will make data on your hard drive unreachable unless they have a password.

- 4. Make Regular Backups.** Ensure that all company data is backed up to a secure offsite storage facility. Thus, even when your systems are compromised, your data will still be secure. The general rule of thumb is that backups should happen once a week. Getting data corrupted is painful but failing to have a backup can be even more painful.

Conclusion. When creating any security measures, the top leadership must lead by example. They must be willing to spend money on programs that help to educate employees. It is important to note that data security is an ongoing process that will require regular revisions.



Shiny New Gadget Of The Month:

Building a Smarter Shower

The cutting-edge U by Moen Smart Shower is looking to revolutionize your shower experience. With digital valves and a corresponding controller, the U by Moen can make any shower a lot smarter.

After users install the digital valves and controller — a task that takes a few tools and a little bit of handiwork — the U by Moen allows them to sync their showers with their smartphone. The system then makes it easy to customize the showering experience, choosing the perfect temperature and saving preferences for future use. Start the shower remotely, and it will let you know when it's ready, automatically shutting off until you step in. Available for showers with either two or four outlets, the U by Moen is the perfect addition for those looking to digitize every aspect of their home.



The U by MOEN

Client Spotlight

CEM Engineering is a thermal power engineering firm founded in 2001 and based in St. Catharines, Ontario.

They have a team of over 35 mechanical engineers, electrical engineers, civil/structural engineers, designers and support staff. They are a leading developer and designer of custom engineered solutions, specializing in the fields of co-generation, energy management and much more.



WasteWater Treatment Plant, Southwestern Ontario



Acute Care Hospital, Southwestern Ontario



(905) 935-5815

www.cemeng.ca info@cemeng.ca

The Canadian Government Says High-Speed Internet is Essential.

As a business owner in Canada, the Internet is crucial to our operations, productivity and success.

How important is the Internet to you?

Would you go as far to say that it's essential for a decent quality of life? Thankfully, the lawmakers in Canada believe it is.

Food, shelter, clothes, and a high-speed broadband Internet connection. Are these the new standards for basic human needs? I honestly think so. After all, it's now the 21st Century, and the Internet has replaced many of the more traditional aspects of everyday life.

The power of the Internet has changed the very fabric of our country. Everything from the decline of cable TV viewership, to the decline of shopping on Main Street. Those who don't have access to a high-speed Internet connection are missing out on more than just Facebook chats and cat memes, they're rapidly becoming second-class citizens.

That's why I was so interested in a news report about a decision made by the Canadian government. **Canadian lawmakers declared that access to an inexpensive, dependable, and fast Internet connection is a basic right for all Canadian citizens no matter where they live. This announcement from the Canadian Radio-television and Telecommunications Commission (CRTC)** came as welcomed news to the 18% of Canadians who live beyond the great technological divide in some of the most remote areas of the country.

Currently, residents in remote areas must pay outrageously high prices for slow and spotty Internet services with low data caps.

Some people pay as much as \$100 a month for 1 Mbps connections. Even for those who can afford to pay the cost, these restrictions prevent millions of Canadians from taking full advantage of all the benefits an Internet connection offers. Expensive and poor-quality Internet connections mean these residents don't have access to critical educational and medical information, nor the ability to conduct business online.

To make matters worse, many of the people in areas without reliable Internet are members of the **First Nations**, who are living in small indigenous communities. Many of them are already facing extreme hardships such as poor food quality, lack of security, and high unemployment. These harsh realities cause widespread feelings of hopelessness, and a much higher than average rate of suicide, especially among young people. Canadian lawmakers hope that by providing accessible Internet to these isolated communities, residents will be able to gain hope and improve their lives.

The chair of the CRTC, Jean-Pierre Blais said, "The future of our economy, our prosperity and our society — indeed, the future of every citizen — requires us to set ambitious goals, and to get on with connecting all Canadians to the 21st Century. These goals are ambitious. They will not be easy to achieve, and they will cost money. But we have no choice."

This goal is ambitious. The government plan calls for all Canadians to have access to unlimited data, with at least 50 Mbps for downloads and 10 Mbps for uploads. The government has already committed \$750 million to the project, and predicts that 90% of all Canadians will have access by 2021.

The Internet in the USA

Right now, in the US, proposed Internet policies that seem intent on destroying net neutrality are working their way through Congress. If passed, these laws would put small businesses at a distinct disadvantage to large corporations that could literally buy up the majority of the bandwidth. This would prevent small online businesses from operating on the same playing field as large corporations.

Besides the possible elimination of net neutrality, US companies still have a long way to go when providing high-speed Internet to all US residents. Even using the FCC's low-bar definition for broadband Internet, which is only 25 Mbps for uploads and 3 Mbps for downloads, millions of Americans don't have access to broadband-speed Internet connections.

According to the 2016 Broadband Progress Report issued by the FCC, 10% of all Americans lack broadband access. This number increased to 39% for Americans living in rural areas. What's even more troubling is that almost half of all American students attend schools that don't have Internet connections with the recommended 100 Mbps per 1,000 students. We can, and we must do better.

This isn't to say that there's no good news when it comes to Internet speeds in the US. Based on a recent report for the first quarter of 2017, the average Internet speed in the US was 18.7 Mbps. That's a 22% increase over the last year and welcomed news for Americans.

In terms of our government, it's refreshing to see that Canadian officials understand the importance of technology to improve people's lives.

Is your business getting the fastest internet service possible?

Contact B4 Networks for more information at (905) 346-4966 or info@b4networks.ca



Adequacy Is Unacceptable

By Robert Stevenson

Recently, while working on a program for a company that has been in business for over 64 years, I came across a particularly compelling value statement: "In the pursuit of excellence, adequacy is unacceptable." It's stuck with me since then as a perfect encapsulation of forward-thinking business philosophy.

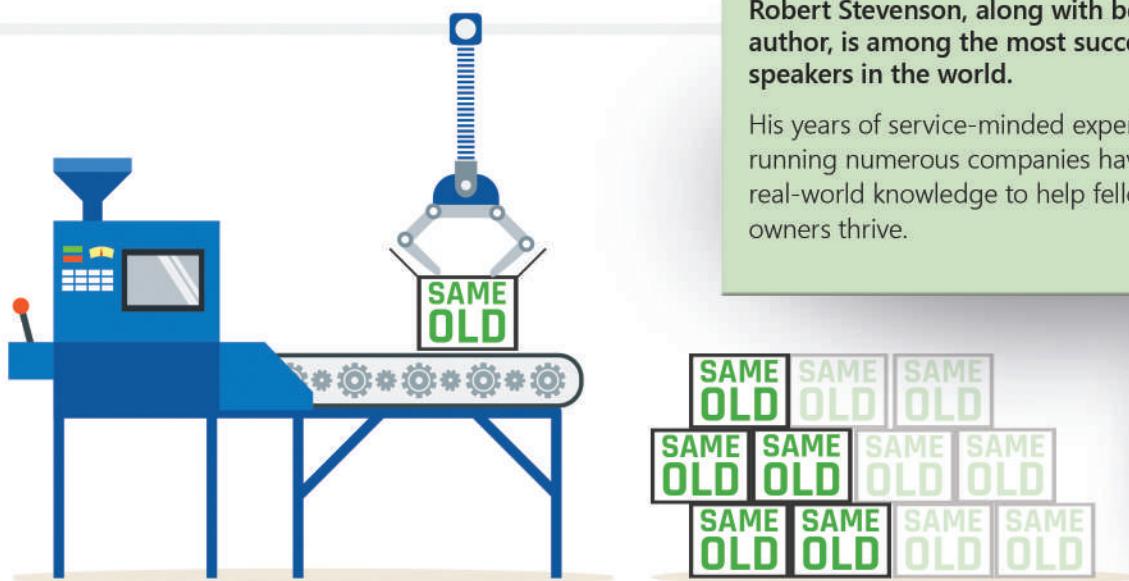
Facebook, Twitter, Yelp, Google, and thousands of other digital tools have completely changed the way companies must do business if they plan on surviving. With two taps on their smartphone, anybody can go online and check out your company. In 10 seconds they can see everything that's being said about you and your team. In an instant, potential prospects can type your company's name into the search bar and sift through your dirty laundry. If people are complaining about your service, your demeanor, or your product, you can say goodbye to this potential customer, because they're moving on. Sometimes, all it takes is a single colorful review to stop us from ever doing business with that company.

So where does "adequacy is unacceptable" enter the mix?

The truth is, people don't go online and write comments about adequate experiences they have with companies. When a customer decides to take time out of their busy day to write a review, you can bet they're going to either rave and rant about their fantastic experience, or go far out of their way to drag your company's name through the mud after the horrible time they had. The smartest companies realize this and bend over backwards to elicit descriptors like "superior," "awesome," "amazing" and "excellent." If your business is doing a middling job, or even a "good" one, it might as well be invisible.

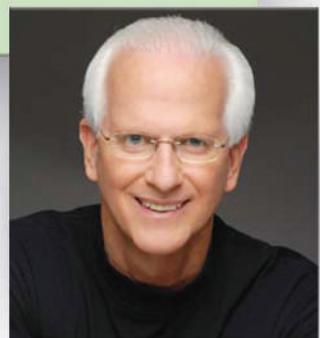
"**Adequacy is unacceptable**" is a perfect ideal not only for the hugely successful business I worked with recently, but for all companies. "Adequate" is just another word for average — are you looking to hire average people or do business with average companies? Of course you're not. The consequence of being merely adequate is always disappointment. An adequate experience captivates no one, does nothing exceptional, and has no distinctive qualities. There is no way to differentiate yourself from the competition while doing an adequate job.

Instead, consider what your company can do to impress, astound and excite those for whom you are working. The company that consistently not only exceeds expectations, but blows them totally out of the water, will always be in high demand. Do more, be more, give more, and you're sure to achieve more. This isn't third-grade soccer; nobody's going to give you a trophy for an adequate performance.



Robert Stevenson, along with being a best-selling author, is among the most successful public speakers in the world.

His years of service-minded experience owning and running numerous companies have given him the real-world knowledge to help fellow business owners thrive.



NEWS BRIEFS

Your Copier Is Spying On You

It may sound paranoid, but it's true: the machines you use every day around the office could be spying on your data.

Copiers and multifunction printers, particularly, are some of the leading causes of business data breaches. When you consider it, it makes sense. They're among the only devices on the network that rarely have their default password changed. But these advanced copiers and printers often house images of all the pages they've ever scanned on an internal hard drive, making them the perfect target for thieves. Make sure to change the password from the default on every network-connected device in your office. This one simple step can save you a costly headache down the road.

intellisystems.com 01/31/2017

**Your Best Employee WILL Quit ... Are You Prepared?**

Employee churn is a fact of business.

It's important to take steps to ensure that regardless of an employee's importance, their loss won't be catastrophic. Consider everyone on your team. If they left, what would it do to your business? Make sure to document indispensable knowledge. In the end, you should keep your team as happy as possible, but be supportive if they make the decision to leave.



Groovehq.com 12/10/15

Fight Traffic Tickets WITHOUT Leaving the Comforts of Home

"Off the Record" is a new app that allows you to contest those pesky speeding tickets without ever leaving your house.

All you have to do is take a picture of your ticket, answer a couple questions, and pay a fee (ranging from \$53 to \$599, depending on your area). The app will then assign the case to a local lawyer to contest the charge. It may sound too good to be true, until you consider its 97% success rate. Best of all, if the ticket is not dismissed, deferred, or reduced to a nonmoving violation, you'll get a full refund!



lifehacker.com 7/7/17

HIGHLIGHTS FOR THE MONTH

September

- Eat an Extra Dessert Day (Sept 4)
- Fight Procrastination Day (Sept 6)
- Star Trek Day (Sept 8)
- International Talk Like a Pirate Day (Sept 19)
- Miniature Golf Day (Sept 21)
- Ask a Stupid Question Day (Sept 28)
- Good Neighbor Day (Sept 28)

NEW EMPLOYEE WELCOME



Britnee Orsini

Words of wisdom: Those who cannot change their minds cannot change anything

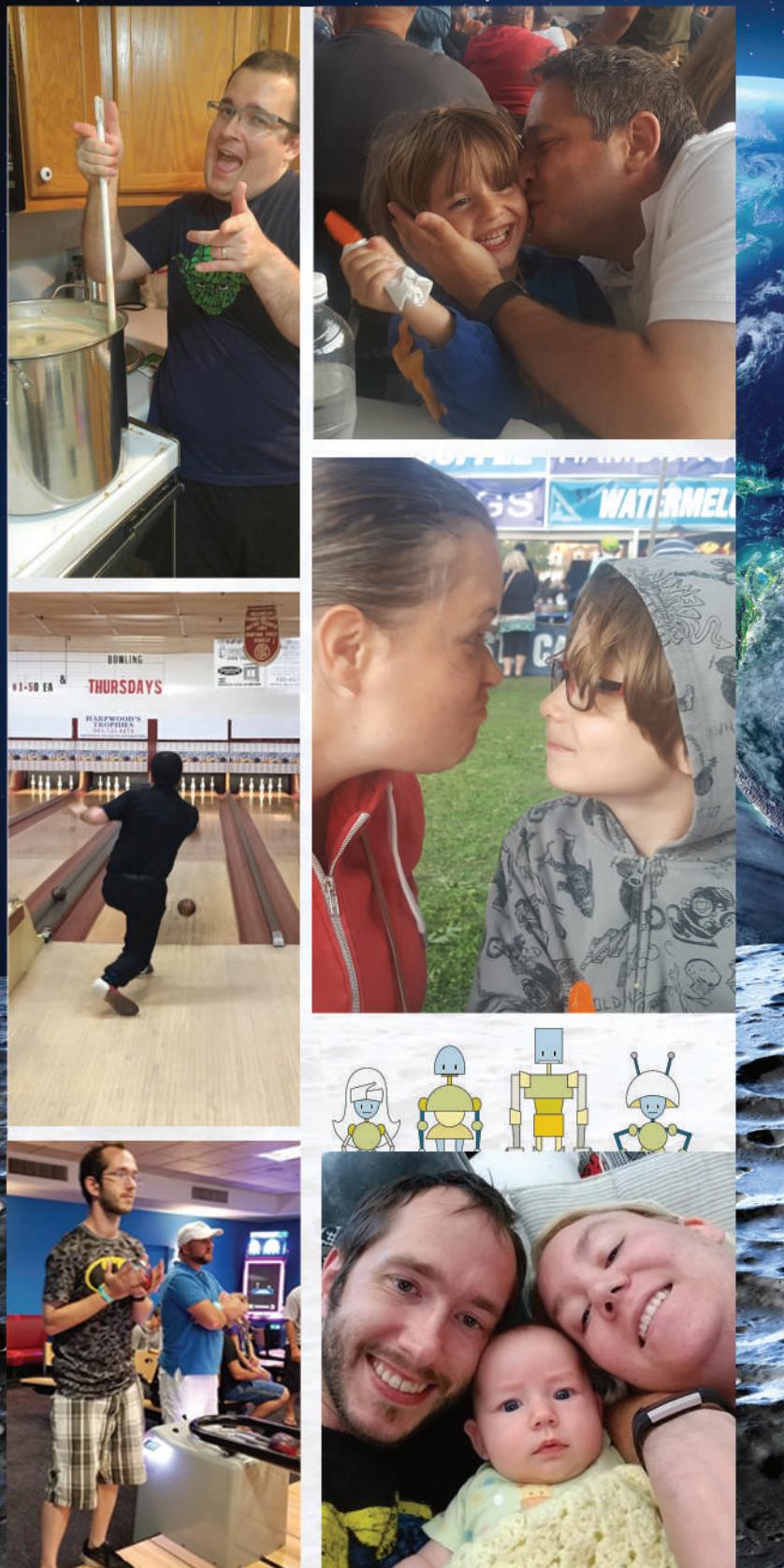
Britnee: Marketing and Office Assistant who is a devoted sports fan, music enthusiast, and animal lover.

Q: What is your favourite food?
A: My favourite food is my dad's homemade pasta

Q: If you could travel anywhere in the world, where would you go?

A: If I could choose anywhere in the world to travel, it would be to Costa Rica and surrounding areas to zipline through the rainforest.

PHOTO ALBUM



TEKTIP

Packing Google Maps, but not an Internet Connection



If you have access to a Wi-Fi connection and space on your phone (300-500mb), you can download Google Maps before you go to avoid cellular data use altogether.

The downloaded maps include local attractions and driving directions between places in areas where those features are available. You can even download the maps at home before you leave for your trip.

To download a map for later use on an iOS or Android device, open the Google Maps app while connected to a Wi-Fi network and sign into your Google Account. Search for the region or location you plan on visiting while on your trip. When the place appears in Google Maps, tap the name in the panel of information next to the map, then tap "Download".

