

This Issue:

Where the Internet Stands in 2018

Do You Know What Your Android Permissions Actually Mean?

Do You Have a Unified Strategy to Your Business' Communications

Is Your Business Considering Moving to Managed IT?

There are New Ways to Secure Your Data

ALERT: Meltdown/Spectre Vulnerability Grants Malware Access, Patch It Today

Hitman Email Scam Threatens Your Life, Instead of Your Data

Do You Know What Your Android Permissions Actually Mean?



Downloading an application on an Android device is fairly simple: access the Google Play store, find the app you want to download, and press the button that says install. However, it is also too easy to simply hit 'Allow' once the app starts asking for ambiguously-worded permissions. Today, we'll examine what these permissions actually mean...



Read the Rest Online!
<https://dti.io/android>

Where the Internet Stands in 2018



People spend a lot of money on the Internet. From an individual standpoint, the amount the average person spends on Internet-based services is their largest expense outside of the money they spend on their residence, and perhaps their transportation costs. In order to understand the landscape of what is effectively a battle for Internet supremacy, you first have to take a look at the battlefield itself.

As of September, of the 7.5 billion people on the planet, nearly 3.9 billion of them (51.7%) use the Internet. In North America, 88.1 percent of people (or roughly 320 million) use the Internet in some fashion. This presents opportunities for thousands of companies. Some provide Internet access to would-be consumers. Some deliver content services. Some deliver applications, computing storage, or processing. This has led to the marketing boom you see on the Internet today; and, is where you find a battle raging between the demand created by billions of consumers, and the companies that deliver the services needed to access that customer base.



A lot of questions have been asked recently about what the Internet is. Questions like:

- How do you monetize access to billions of potential customers?
- Should Internet access be free?
- Is Internet access a utility (and thus governed by different rules)?
- Who is in charge of the Internet?
- What is the Internet of Things?

Questions like these produce a variety of answers. With the smoldering embers of the U.S. net neutrality laws suggesting further corporate control of the Internet, we'll look at the way the Internet is set up in 2018, the costs for businesses and individuals, and why the companies that control access to the Internet are licking their proverbial chops; and, how it challenges the core interpretation of what exactly the Internet is.

The Internet in 2018

The Internet has come a long way in a short time--so far it seems, that it's hardly recognizable
(Continued on page 2)

Do You Have a Unified Strategy to Your Business' Communications



Communication is one of the cornerstones on which your business functions, and without it, you will find that going about your daily duties is considerably more difficult. Communication is one of the many ways your organization accomplishes both major and minor tasks, so you want to pay especially close attention to how your business handles phone calls, email, and even mobile devices--both in and out of the office.

Unified communications include several solutions that your organization can use to stay connected, including a unified email solution, mobile device strategy, and a telephone solution. All of these types of solutions should be built around today's expectations of mobility and flexibility. Here are some of the ways your business can build out a unified communications system that improves connectivity.

Email

Email has long been a staple of

business, but how do your employees use it? Do they access it on multiple devices? Do they use the same email service (Hint: They should)? An employee who prefers Gmail over Microsoft Outlook might decide that they would rather use the solution they are most comfortable with. This is an issue, as it spits in the face of your attempt at unified communications.

Email is most useful when it's kept to your preferred email solution, so you should ensure that your organization is prepared to spend time on training employees how it works. The solution you choose should be one that can be used on several different devices so as to provide your employees with maximum choice in how they use the email system. If you're worried about hosting your email server, Directive can help you out with that, too.

Mobile Device Management

Mobile devices are all over the place now, and your business could benefit from having them become a part of your infrastructure. However, they need to be managed properly, as the more apps have access to your business's data, the more exposure it gets to potential threats. You need to make

sure that you're prepared to handle this influx of mobile devices if you're hoping to provide a truly unified communication infrastructure for your organization.

Beyond compatibility, you want to make sure that your organization is prepared to handle lost or stolen devices, fraudulent apps, and other security risks. Directive can help you whitelist and blacklist apps, as well as remotely wipe lost or stolen devices. This helps you keep your data as safe as can be.

Unified Voice over IP

Traditional telephone solutions don't take the flexibility of the modern business in mind. Landlines tend to bundle together services with little flexibility, leading to organizations overpaying for services that they don't need. If you're paying for services that you don't need, you're wasting assets that are better spent elsewhere. Furthermore, you're limited to taking calls on your work phone in your office, hampering your ability to be productive while out of the office or on a business trip...



Read the Rest Online!
<https://dti.io/unified>

Where the Internet Stands in 2018

(Continued from page 1)

ble. The Internet of 2018 will continue to be the predominant marketplace in the world. It is seemingly in the process of being consolidated. In fact, 50% of Internet traffic in North America is from 35 websites. In 2007, that same amount of traffic was spread around several thousand websites.

Whether or not a handful of companies own most of it is irrelevant to a consumer, but it's getting to the point where the product is so consolidated that prices will almost assuredly increase. It's like Gap Inc. They own The Gap (obviously), Old Navy, Banana Republic, J Crew, H & M, and a few other companies that do largely the same thing: manufacture and sell clothes.

Each of these retailers has its own branding and its own management teams, but the money goes to the same place.

The Internet, for all its vastness and entrepreneurial promise, is seemingly controlled, like many industries in the United States, by heavy hitters--companies like Google, Amazon, Facebook, etc. Without playing by their rules, many companies may as well peddle their wares from a kiosk at the local mall. 80% of referral traffic comes from Facebook and Google. This is why many retailers' sustainability is tied to how they are able to properly advertise their product...for these two company's search algorithms. Today, tens of thousands of marketing companies have

supplied the immense demand to build constructs that meet the demands outlined by the masters of the Internet.

The Cost

The Internet is extremely important to us. Our business, and our clients' businesses, rely on it every single day. We aren't alone, and in many ways, the Internet is the newest (and arguably last) frontier. If something were to happen and the Internet were to go out for an extended period of time, tens of thousands of businesses, including ours, would likely cease to be. The truth is that we'd pay what we'd...



Read the Rest Online!
<https://dti.io/stand>

Is Your Business Considering Moving to Managed IT?



Your business relies on its technology being maintained properly, but it's not always as simple as up-

dating a software application or replacing a hard drive following a catastrophic failure. You have to think about who you're paying to maintain your technology solutions, if there's anyone doing it at all. You need to consider what happens when you lose data or when your organization experiences downtime. How do you keep technology from becoming a hindrance for your business? Managed IT is one of the best ways your organization can capitalize on its technology without worrying about whether or not you're maintaining it properly. The ideal way for a small

business to manage its technology is to have professionals handle it while you focus on other aspects of the management process.

"Managed IT is one of the best ways your organization can capitalize on its technology without worrying about whether or not you're maintaining it properly."

In other words, let's ask you a question; is your business running as smoothly as possible? Can you honestly say that you have time in your day to handle multiple technological troubles, as well as all of your other responsibilities? Upper-level executives like the CEO and COO have other responsibilities that are more pressing, and as such, technology maintenance is often left to your employees, who may (or, more likely, not) know what they're doing. Technology

maintenance is something that should always be done by professionals, as any mistakes could become costly mistakes that lead to downtime caused by having to do the same work twice, or even your technology failing completely.

Imagine what would happen if a hardware failure occurred and you lost the entirety of your business' data. What would you do then?

Instead of relying on your employees, who have other jobs to do as well, managed IT can make sure that your organization's technology is always maintained. Since a managed IT provider like Directive is dedicated to maintaining your business' technology, you won't have to worry about other tasks...



Read the Rest Online!
<https://dti.io/managed>

There are New Ways to Secure Your Data



Security is an aspect of running a business that absolutely cannot be ignored, regardless of whether or

not you see it as a considerable issue in the near future. The fact remains that your organization will always be at risk unless you take actions to keep it safe today. By taking advantage of some of the latest and greatest security tools on the market, you'll be able to protect not only from the basic threats, but more advanced ones as well.

No matter how advanced technology becomes, it can fall victim to even the most basic of threats if left unchecked. Your desktop workstation is certainly not immune to threats like viruses, malware, spam, and so much more, and even the most vigilant business could expose its infrastructure to these common threats. Since consumer-grade services are likely not strong enough to

protect your business's important data, you'll need to turn to enterprise-grade solutions that can be tricky for small businesses to afford.

One of the greatest ways you can protect your organization is by implementing a Unified Threat Management tool that fulfills the roles of various security solutions in one convenient package. For example, you could implement an enterprise-grade antivirus and firewall to keep threats out of your infrastructure and promptly eliminate those that do infiltrate your defenses. Furthermore, preventative solutions like spam protection and content filtering can limit your organization's exposure to threats in the first place, which saves time and money in the long run.

More advanced security protections, however, are certainly important for your business as well. Some of the more powerful measures include two-factor authentication and biometric scanning. Two-factor authentication is particularly important, as it provides a secondary credential that must be used to gain

access to important information and accounts. Basically, it forces hackers to do even more work to break into an account, as they would have to physically steal your smartphone or other device to which the secondary credential is being sent to, all just to access an account and maybe find something useful.

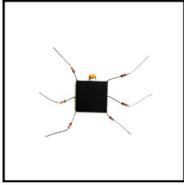
Biometrics, on the other hand, are a bit harder to fake. Using fingerprint scanners or iris scanners make it considerably more difficult to unlock devices. A hacker would basically have to have the exact same fingerprint or iris as you, so unless there is some incredibly shady business going on, they won't be able to access your devices.

How does your business secure its sensitive information and data infrastructure? Directive can help your business avoid considerable security troubles. To learn more, reach out to us at 607.433.2200.



Share this Article!
<https://dti.io/secure>

ALERT: Meltdown/Spectre Vulnerability Grants Malware Access, Patch It Today



Mere months after the firmware in their computer

chips was found to be seriously flawed, Intel's flagship product has once again brought some unpleasant attention to the company. While the issue now has a fix, there was the possibility that a solution could depreciate the functionality of the CPU.

In a blog maintained by a user known only as Python

Sweetness, a post went up stating that "an embargoed security bug impacting apparently all contemporary CPU architectures that implement virtual memory, requiring hardware changes to fully resolve."

In layman's terms, there was a bug that interfered with how other programs interacted with the CPU. A functioning CPU has two modes, kernel and user. User mode is the one that is generally considered 'safe' mode, while kernel mode grants access into the

computer's inner workings. Python Sweetness, however, realized that there was a bug that blurred the lines between user and kernel mode. This issue created a means for malware and other malicious programs to access a system's hardware directly.

This bug was expected to cause the system to have to switch entire processes back and forth between user mode and kernel mode, which...



Read the Rest Online!
<https://dti.io/spectre>



Chris Chase
Solutions Integrator

Hitman Email Scam Threatens Your Life, Instead of Your Data



Email scams have become a sort of punchline, often

featuring Nigerian princes or wealthy, unknown relatives in need of funds to get home. However, another email scam is anything but amusing, as it uses a unique possession of the target to entice them to comply: their life.

This email appears in the target's inbox with the subject line "Please read this it can be the most important

information in your life," a clear example of clickbait. However, the story that unfolds is worth accessing the email--or at least, it would be, if we weren't going to tell you the story here.

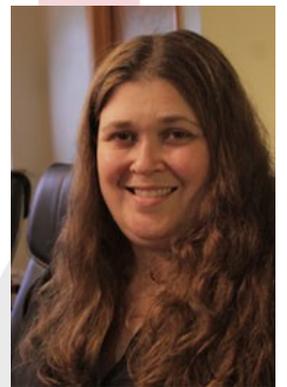
Once opened, the recipient will find a message that suggests a great drama is unfolding on the periphery of the recipient's life. According to the email, the recipient has had a contract put out on their head, the sender of this message being the hitman who is charged with taking them out. As the email says, "I

received an order to kill you, because your activity causes trouble to a particular person."

However, in a twist of events, the contract killer has decided to give their target the opportunity to save themselves after studying them. This is clearly a big deal, as the "business rules" of his or her profession do not allow this kind of activity, and so sending the target this...



Read the Rest Online!
<https://dti.io/hitman>



Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com



newsletter@directive.com



facebook.directive.com



linkedin.directive.com



twitter.directive.com



blog.directive.com



instagram.directive.com

