directive

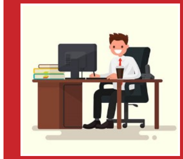
TECHMinutes

August 2018

Your Small Business Technology Information Source!

This Issue:

Keep Employees Off of Distracting Websites



As incredible a tool as the Internet truly is, for every website that is beneficial to the workplace, there is another that is certainly the opposite. Naturally, it is these sites that your employees would most likely want to visit if left to their own devices. Sometimes, the best course of action is to remove the temptation and block these websites. For this week's tip, we'll talk about a few ways to do so.

Block Websites from the Network

The most basic way to block your employees from accessing websites is to block these websites from the entire office network. To do so...

Read the Rest Online!
https://dti.io/focus

25TH ANNIVERSARY
est. 1993

Should High-Speed Internet Access Be a Luxury?

With so many new technologies being introduced and innovation at the highest levels in human history, you'd think that ubiquitous access to bandwidth Internet would be high on the list of the priorities of ISPs and for residents of every jurisdiction. This doesn't seem to be the case. With the disparity between urban and rural bandwidth Internet offerings growing by the day, we look at the causes of the gap and how companies plan on getting Internet access to people in areas where the population may be low.

A little background would tell you just how much some places are behind others. To start, 15 million Americans don't have access to broadband Internet. Beyond that, they pay more for it than almost any people in a first-world nation; and, if that wasn't enough, the average speed available is slower and less reliable. Furthermore, it seems as if the Federal Communications Commission, the federal regulator of such things, finds no problem with this--and if there was a cherry on top, they seem to be foregoing assessment and analysis of the problem for more nationalistic rhetoric stating that new strategies that have been implemented after the fall of net neutrality laws are "removing barriers to infrastructure investment, promoting competition, and restoring the longstanding bipartisan light-touch regulatory framework."

This despite two FCC commissioners saying things like the FCC's statement is "ridiculous and irresponsible," and "biased, flawed, and woefully incomplete." The politicization of what traditionally is an objective report, is one of the many problems that the people of the United States are facing in regard to Internet availability. Unfortunately, this has been an ongoing problem for the better part of two decades. Let's move away from politics to look

(Continued on page 2)

Cloud Can Cover Most of Your Business Needs

The traditional computing structure has been under siege by cloud computing for the past several years. More businesses than ever are seeing the value in cloud-hosted applications and infrastructure, and while that may not be a huge surprise, the perceptions that the cloud can solve any of your organizational computing problems depend largely on the needs of that endeavor. Today, we will take a look at successful small business cloud strategies and tell you why they find success.

Cloud for File Sharing

File sharing is the number one reason any small business moves some of their computing to the cloud. Cooperation is essential to small business success, and a cloud-based file sharing solution gives any small business near-ubiquitous access to data. This access allows work to be completed from multiple locations, giving the small businesses great benefit as it makes them competitive with larger organizations who have more people and more resources. This allows small businesses to take charge over more of the market than ever before, increasing revenues and promoting business growth.

Cloud for Communications

Another avenue a lot of small businesses are taking is using cloud-hosted communications services. Like many other cloud-hosted applications, it can save a company quite a bit of

(Continued on page 3)

How the IoT Can Be a Security Risk

The Internet of Things means a lot more than just enhanced connectivity. In particular, you'll have a considerable security risk associated with the Internet of Things. It's clear that the more devices accessing a network, the more risk will be associated with that network, which is where the inherent risk of the Internet of Things comes into play. How can you control the number of devices accessing your network, and thus secure your business from the Internet of Things?

Understanding why security is such an issue for Internet of Things devices is critical to keeping your business secure from these devices.

Too Many Devices

The more threats are associated with a particular industry, the more likely you'll encounter a threat. This is not conjecture--it's reality. When you consider how many devices now have connectivity compared to the past, you might realize that these fears regarding the Internet of Things aren't unfounded. You should go about organizing your business' security by imagining what you would do in a worst-case scenario in which at least one of these devices makes it past your organization's defenses. All it takes is a single weakness to bring down an entire network.

> ***"The Internet of Things means a lot more than just enhanced connectivity."***

The issue with these devices is that they are often those that you wouldn't expect to traditionally have such connectivity. For example, you might not immediately think of cars, kitchen appliances, watches, or thermostats to have such functionality. These can be difficult to plan for if you're not careful.

Patches and Updates

When there are a lot of devices accessing a network, chances are that at least one of them won't be up to snuff with its updates and patches. The incredible vastness of the Internet of Things all but guarantees that at least one of these devices is going to be out of date, placing your organization at risk. To make things even worse, some Internet of Things devices are created based off a trend that could very well be obsolete soon afterward, meaning that developers might not see the need to support the device beyond that timeframe. For example, if a device sells poorly and was created only to meet specific...

Read the Rest Online!
https://dti.io/iotsecurity

Should High-Speed Internet Access Be a Luxury?

(Continued from page 1)

at some of the ways that the country is making out with Internet access.

Internet Service Providers

An Internet Service Provider (ISP) is a company that, well...provides Internet service and support to customers. ISPs don't have to be huge media conglomerates, but many of them are, and while they mostly provide in-home service, and "business-class" service, they do a lot more than that: they provide an essential service to everyone that needs it. It doesn't seem like there is any difference in the two, of course, but there is. It is this qualification that allowed FCC chairman Ajit Pai to effectively take down the net neutrality laws in 2017. It was all in the name to allow ISPs to be looked on as less of a utility (which they most certainly are) and more as a service; thus, paving the way for infrastructure investment.

So, in layman's terms, the ISPs needed incentive to build access to Internet where it wasn't, and have been given the run of the Internet to make this happen. That would be great if ISPs, especially the major ones, had a strategy in place to make these infrastructure investments, but it seems, at least on the surface, that the only thing they did have a strategy for is to reap the benefits of the dissolution of the net neutrality laws.

No matter how you slice it, the ISPs that distribute broadband access in the U.S. (and in the U.K. for that matter) aren't doing a great job at serving their customers. As of May 2018, the United States ranks 47th in the world in average bandwidth speed, while the U.K. ranks 51st. At the same time, only four nations' businesses pay more for high-speed Internet than businesses do in the United States (at $60.14 per month). At least in the U.K. the average price for high-speed Internet is under $37 per month ($36.83).
If those figures weren't bad enough, before the newest era of deregulations, ISPs have been accused of pocketing hundreds of millions of dollars for fiber optic infrastructure that never materialized. Skeptics say that most of that was tax subsidy and it was utilized in creating many of the wireless networks that we all utilized today. So, whether or not the ISPs did, in fact, invest that money back into infrastructure or not, many people would argue that it was not what that money was appropriated for and that it should be a giant scandal. Since it wasn't, it's fair to assume that the truth is somewhere in the middle as many of these investments were made before the great recession at the end of the last decade. Besides a lot of that capital would have been going to state utility telecommunications contractors and not the ISPs themselves. If ISPs need public assistance to lay this infrastructure it stands to reason that the public should get some of the benefits. Of course, this isn't the case and it just makes the ISPs positioning in this case seem awful questionable...

Read the Rest Online!
https://dti.io/highspeed

Cloud Can Cover Most of Your Business Needs

(Continued from page 1)

money switching to a VoIP system or public-cloud-hosted email solution. What about functionality? Cloud-hosted VoIP is actually a great solution for any organization looking for a feature-rich phone platform and wants to do away with their traditional phone bill. With feature-rich packages, any organization can get the customized VoIP solution that fits in their budget and provides them options for messaging, conferencing, and enterprise-level phone services.

Hosted email can provide a lot of benefits, as well. It eliminates the costs associated with the hosting and management of the email server, while providing users enhanced functionality that includes added message encryption, instant messaging integration, and much more.

Cloud for Storage

When you think about cloud storage, the first thing that must come to mind are the hundreds of gigabytes that many cloud storage providers just give away to anyone that signs up for their services; and the affordable options individual users can explore to gain a substantial amount of cloud storage space. The issue for small businesses is that public cloud hosted storage facilities don't provide them the control over their data that most of them would like. This is why you see organizations building their own private cloud inhouse or collocate it to a data center where they have full control over the data.

The benefits of cloud storage are that data is accessible from anywhere, giving a business increased mobility that can definitely benefit them over time. The perceived lack of security that some organizations point to is largely in how their employees utilize the cloud interface, not the cloud environment itself, as it is likely highly encrypted. Many organizations have begun to use cloud storage interfaces for redundancy, making cloud-based backup and recovery solutions a fairly attractive option to secure backup files.

Cloud for Security

Nowadays, security is the top line-item for about any IT administrator. Since there is an abundance of threats every organization has to be cognizant of, it only makes sense that cybersecurity firms start offering their comprehensive network and cybersecurity services. In utilizing a SEaaS system IT administrators can leverage some of today's most potent security solutions from the…

Read the Rest Online!
https://dti.io/cloudcover

Understanding RPO and RTO

Data backup. Nobody wants to think about it until it's too late to do anything about it. While no business ever hopes that they will be struck by a data loss incident, no business will ever regret implementing a backup on the off-chance that they ever suffer from a worst-case scenario. What are some of the most important parts of a data backup and business continuity system? We'll start with Recovery Point Objective and Recovery Time Objective.

While they might sound similar, RPO and RTO are two very different things that work toward the same ultimate goal of sustaining your business' continuity in the event of some catastrophe.

Recovery Point Objective

When you picture your business suffering from a data loss incident, just how much data do you see yourself losing? Whether it's a considerable amount of data or just a couple of files, we want you under the impression that no amount of data loss is acceptable for your business--particularly because you can never know if that information will be restored again or not in the future. Your ultimate goal should be to minimize data loss by any means necessary, which leads us into the recovery point objective.

> ***"Data backup. Nobody wants to think about it until it's too late to do anything about it until it's..."***

Basically, the Recovery Point Objective is a designated amount of data that your organization aims to restore in the event of a disaster. It's ideally 100%, and most modern backup solutions will help you reach this threshold. Incremental backups like those taken with a comprehensive Backup and Disaster Recovery (BDR) solution can help you toward this end.

Recovery Time Objective

The other half of BDR consists of the recovery time objective. How long does it take your business to recover in the event of a disaster? The idea is to minimize this time, as downtime can be both expensive and risky for your organization. Any time when your business isn't functioning as intended due to data loss or otherwise constitutes downtime, and situations like these are costly--meaning that you should minimize them as often as possible.

Business continuity needs a minimal recovery time objective so that you can get right back in action following a data loss incident. The best way to accomplish this is through a Backup and Disaster Recovery (BDR) solution from Directive. You can minimize data loss and restore your data backups directly to a temporary device so that your business doesn't have to wait any longer than needed to get back in action. To learn more, reach out to us at 607.433.2200.

Share this Article!
https://dti.io/rpoandrto

Reexamining Meltdown and Spectre

It's been about a year and a half since the Meltdown and Spectre exploits became publicly known. While patches and updates were administered to reduce their threat, they continue to linger on in a less serious capacity. Of course, this doesn't mean that the threat has entirely been neutered--you still want to know what these threats do and whether or not you're safe from them.

What They Do

The Meltdown and Spectre threats both target the system processor, though in different ways. Meltdown essentially melts away the barrier between the processor and application processes and the system memory. On the other hand, Spectre can fool the processor into accessing parts of the system memory that it's not supposed to. Both of these threats allow unauthorized access to a user's system, creating more opportunities for further threat influence.

The biggest problem with Spectre and Meltdown is how widespread they are. They could potentially cause problems for every computer chip created over the past 20 years. Consequently, any data stored by technology utilizing these chips is also at risk.

How These Issues Were Resolved

Meltdown and Spectre have no definitive fix at the current moment, even though patches and updates have been frequently released in order to combat the latest updates to this threat. When the patches were first developed against Meltdown and Spectre, developers foresaw a major decrease in performance on the user's end--as high as thirty percent, in fact.

Even though these patches do influence performance, the difference isn't nearly as much as it was initially predicted to be. Depending on the individual circumstances (outlined below), the average user encountered much smaller effects that didn't exceed five percent. Of course, this could change with future patch releases, but it's important to keep in mind that the initial patches are generally going to have the biggest effects, as the primary concern is resolving the security issues rather than improving performance right off the bat.

What Influences Performance?

There are several factors that can influence the performance of your system following the patches of Meltdown and Spectre.

Use

Depending on what you use your system for, Meltdown and Spectre will have different effects on your system performance. It's reasonable to assume that applications and uses that need more processing power will be affected more than other processes. If you take advantage of virtualization, or are investing in cryptocurrency mining, chances are that you'll see a performance drop as a result of these patches.

Patch Used

Several companies have issued patches for these threats, so naturally you'll have various effects from them.

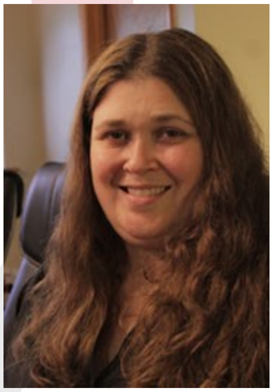
Device Configuration

Your hardware and software configurations are going to change how much your...

Read the Rest Online!
https://dti.io/meltspec

25TH ANNIVERSARY
est. 1993

Chris Chase
Solutions Integrator



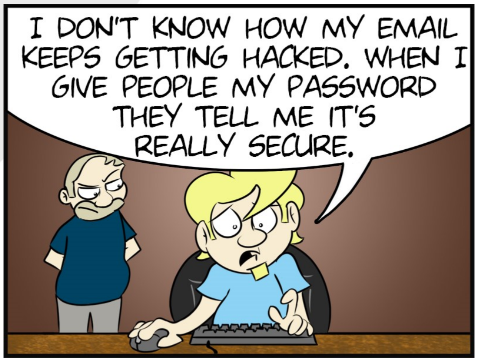
Charlotte Chase
Solutions Integrator

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


I DON'T KNOW HOW MY EMAIL KEEPS GETTING HACKED. WHEN I GIVE PEOPLE MY PASSWORD THEY TELL ME IT'S REALLY SECURE.