TECHMinutes

September 2016

Your Small Business Technology Information Source!

This Issue:

Protect Your Online Identity With These 8 Tips

The Internet has long been a great tool for business, but you can't take advantage of it without putting your sensitive data at risk of threats, like hackers and malware. Granted, when it comes to cyber security, even the most cautious business will have a lot on their plate. We'll go over eight of the...

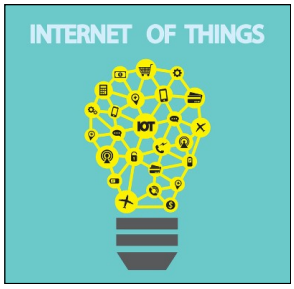
Read the Rest Online!
http://dti.io/protect

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us online at:
newsletter.directive.com

The Explosion of Mobile Devices is One Trend Your Business Must Account For



You may have heard about the Internet of Things in passing, but do you truly understand the nature of these connected devices, and how they will affect your business in the coming years? The Internet of Things is a major trend that needs to be addressed if your business plans on succeeding in the near future.

Gartner reports that by 2020, there will be approximately 21 billion devices connected to the Internet; an astounding number, and one that your business can't afford to ignore. These devices could range from fitness devices designed to track vital signs like pulse and heart rate, to connected appliances like refrigerators, thermostats, baby monitors, security cameras, and so much more. The sheer utility that the Internet of Things provides, guarantees that it's only a matter of time before your office has to deal with several similar devices.

In fact, we'd be surprised to hear that your business doesn't have at least a few of these devices floating around your network, especially considering how most of them are consumer-targeted, and are perhaps in the possession of your employees. Even something as simple as a smart watch could make its way to your business's infrastructure, and unless you're monitoring which devices connect to your network, you'd

(Continued on page 2)

3 Ways Help Desk Support is Perfectly Suited for SMBs

Let's say that your team is deep within the throes of productivity on a major project, and even the slightest hiccup will knock off their momentum and derail all progress. What would happen if the software they need to do their job suddenly became unusable, or settings on their workstation get changed without their knowledge? Without a reliable IT department, you might be out of luck.

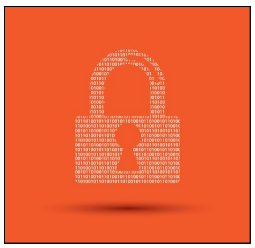
Consider, for a moment, what could happen if you let your employees service their own computer, or work on things without any oversight whatsoever. What if they accidentally misplace data, or remove a component that's critical to the functionality of their workstation? The possibilities for something to go wrong are limitless. This is why you only want knowledgeable technicians working with your solutions.

However, what if you don't have it in your budget to hire an experienced IT technician? There remain several opportunities for small and medium-sized businesses that may (or may not) have an internal IT department. Directive's help desk solution is among them; it's capable of providing your team with the support it needs to keep operations moving forward. We can act as your outsourced IT department, whom you can contact at any time should support be needed.

Here are just a few of the many benefits that come with Directive's help desk solution:

(Continued on page 3)

Having a Network that's Tested Guarantees You'll Overcome Any Disaster



Does your SMB have an internal IT department? Chances are that it is a major pain point for your organization, and even if you do have one, it might be bogged down with so much work that mistakes can happen and threats can slip through the cracks. Sometimes the best way to protect your network is to know where and how threats manage to get there in the first place.

At Directive, we call this type of preventative measure "penetration testing." It's designed to test your network for any outlets that can be exploited by hackers or other threats that want to do harm to your network systems. This could include testing your workstations for vulnerabilities, ensuring that all of your software and hardware is up to date, and examining any mobile device usage on your network. As such, it's a critical part of maintaining a safe and healthy network infrastructure.

Penetration Testing Also Means Testing Your End-Users

With network security, one of the often-ignored outlets for a blah blah threat infiltration stems from the end-user. If they accidentally hand over credentials, or download a malicious file off the Internet, you could be looking at a virus or malware takeover. In a worst-case scenario, they could walk into a phishing scam and have your entire system encrypted by ransomware. The ransomware could be Cryptowall, and the entire infrastructure could be encrypted with military-grade encryption, forcing you to either pay up or restore a backup.

All of these situations can be avoided if you properly train your employees on how to avoid online threats. Many security best practices are common-sense, but it helps to provide a refresher on how best to approach threats to security. Regularly quiz your employees on what to do if they encounter a potentially dangerous situation, and emphasize the importance of data security in your corporate culture.

Plan for Possible Scenarios

One of the best ways that you can protect your infrastructure is putting together emergency management plans for how to handle specific scenarios. This way, your organization won't be caught off-guard by unexpected disasters that have the potential to derail your operations. Here are just a few examples of situations you'll want to prepare for:

- Hacking attacks
- Data loss
- Natural disasters
- Hardware failure
- Other downtime-causing situations

Is your business prepared to handle the burden of network security, and can you protect your network from the many threats that lurk on the Internet? Your business doesn't have to suffer at the hands of unplanned disasters. To learn how your business can better prepare for the future and keep threats out of your network, reach out to us at 607.433.2200.

Share this Article!
http://dti.io/netdisaster

The Explosion of Mobile Devices is One Trend Your Business Must Account For

(Continued from page 1)

never know (until something goes wrong, of course).

Perhaps the most dangerous part of Internet of Things devices is the fact that they not only connect to the Internet, but that they are also able to communicate with each other. If these devices share your business's corporate information with unapproved devices, you could have an unintentional data leak that exposes sensitive data to malicious entities.

In order to counter this potentially disastrous occurrence, it's important that your business understands how to work mobile devices into your network infrastructure. You can't just let anyone connect their personal devices to your network. What if one of them were infected with malware, spyware, or other threats with malicious intentions?

With a Bring Your Own Device (BYOD) policy, you can set up rules that govern how users take advantage of Internet of Things devices in the workplace. You should aim to have only approved devices connecting to your company's network. The goal is to restrict your business's network to only devices that won't compromise its integrity. Users should first inquire about the devices they would like to use in the office, and once they've been approved by IT, they can begin to use them; but only if they aren't a threat to productivity or data security.

Furthermore, some mobile devices, like smartphones, can be used while out of the office to stay productive and connected to the workplace. These devices need to be managed so as to protect the integrity of any data stored on them. This includes whitelisting and blacklisting apps, as well as allowing for remote wiping. Doing so effectively allows you to manage risk and take matters into your own hands, should your policies not be enough.

To learn more about how to manage risk with Internet of Things devices and other mobile technology, call us today at 607.433.2200.

Share This Article!
http://dti.io/iotdevices

3 Ways Help Desk Support is Perfectly Suited for SMBs

(Continued from page 1)

Convenient support

With a help desk solution, you can have near-constant access to technical support for your business's mission-critical systems. If your team needs help with an issue, we're here to help walk them through it. Our team can even remotely access your systems and resolve the problem, which cuts out the expense of an on-site visit, and resolves the issue quickly and efficiently.

Assistance from professional techs

One of the greatest benefits you get from working with our help desk is that you're not receiving support from some hack halfway across the world; you're instead working with someone who has a working relationship with your business, and someone who is invested in the success of your organization. We succeed when you succeed, so we're always happy to go the extra mile for our clients.

Single point of contact

Nobody likes to deal with vendors, and it can be an excruciatingly painful process when your organization has to contact multiple vendors just to troubleshoot a technology component. Instead of reaching out to each one individually, you can contact Directive, and we'll act as a single point of contact so that you can keep operations pushing forward.

Does your SMB have the technology support it needs to ensure maximum efficiency? IT management and maintenance isn't something that the average office worker should be handling; you want only the best and brightest minds caring for your hardware and software solutions. Directive can provide you with the tools and services you need to succeed. To learn more about our help desk solution, or to ask about our other outsourced IT services, reach out to us at 607.433.2200.

Share this Article!
http://dti.io/helpdesk

We Debunk 3 Common Myths of Managed IT

Managed IT services are so popular with small businesses that they're becoming a commodity. If you're not taking advantage of managed IT, what's your excuse? Here we address three common excuses put forth by companies that avoid managed IT.

"I'll save money by only fixing technology when it's broken."

At first glance, this seems to make sense. By only performing maintenance on your devices when they aren't operating as intended, you should be able to save money in the long run. The only problem here is that technology by nature requires that you perform maintenance on it regularly in order to maintain optimal performance. If you aren't providing the care that it needs, you're holding your business back from achieving its maximum potential.

Then you have to consider the fact that technology is much more expensive to replace outright than it is to perform routine maintenance on. Think about it; a server unit is very, very expensive, and so are good, quality workstations. If you're going to purchase hardware, wouldn't it make sense to perform maintenance on it and guarantee a long life, rather than await a premature hardware failure? Managed IT seeks to provide this care throughout the lifetime of your technology to ensure its longevity and proper functionality.

"My technology doesn't need maintenance regularly."

Some businesses are under the impression that they don't use their technology enough to justify regular maintenance routines. This may be because they only use their office productivity suite, the Internet, and not much else. If technology systems don't receive regular maintenance (like patches and updates), security can quickly become a problem. Also, when you don't experience a targeted hacking attack, it can be easy to fall into a false sense of security.

Then there's the problem that comes from having Internet-connected hardware like servers and workstations. Most businesses will be using their technology solutions to browse the Internet and conduct business with email and other communications which could potentially result in a data breach. Do your employees know how to identify phishing scams and other online malicious activity? While most organizations use security solutions like firewalls and antivirus, consumer-grade is often not enough to protect sensitive data from hackers and data breaches.

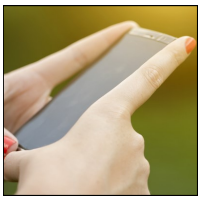
"My employees and I can handle IT all by ourselves."

Here's one of the biggest reasons why companies don't implement managed IT services; they feel that they can do a fine-enough job managing their own technology. This is fine if companies have an internal IT department, but it's more likely that small businesses are relying on their own employees to perform troubleshooting procedures and basic tech maintenance to save money.

Ask yourself this question: "Would I rather have skilled technicians working with my technology, or my busy employees, who have other duties and obligations?" More likely than not, you'll want your team to focus on their responsibilities within your organization, rather than wasting time with your business's technology. Managed IT allows your team to take a step back and focus on what matters most: your business.

Share this Online!
http://dti.io/itmyth

Just Because an App is on the Google Play Store, Doesn't Mean it's Safe



If your employees are given an Android device to use for work, or if they bring in their own as a part of BYOD, you may want to pay special attention to what follows.

Google has just removed a piece of malware that managed to make its way into the listings of the Google Play Store. Disguised as a strategic card game called "Beaver Gang Counter," the malware seemed at first glance to be a harmless enough app to download as a way to pass some time every now and then. This impression unfortunately turned out to be inaccurate for a few different reasons.

So Why Was it a Threat?

First, the app itself reportedly was a bit of a one-trick pony, losing any of its entertainment appeal very swiftly. Of course, what does one do with an app that one has grown bored with and no longer wants? One deletes it, to make room for other apps that one will have more use for, but not before the second factor that makes the "harmless" impression inaccurate comes into play.

The disguised malware would specifically target those whom also had Viber, the vastly more popular communications app, installed on their device. Once the Beaver Gang Counter app was installed, the malware would access the directories contained in Viber as well as uploading any of the user's Viber images to an external website.

Google has since denied Beaver Gang Counter from the Play Store, and thus far it seems that little damage was done. However, the entire situation asks the question: how did this happen?

There were ultimately a number of factors that led to Beaver Gang Counter having the ability to access files belonging to another app - an ability that the Android platform is supposed to block. However, the measures put in place by Android do nothing to prevent the review of data saved on the SD removable storage.

Due to the expectation of inter-device compatibility that comes with SD cards, the inter-app file sharing that Android usually blocks is left unfettered in the SD storage, depending on the permissions granted at install. Therefore, if assigned to SD memory (as it would have been in almost all cases), Beaver Gang Counter could potentially access any and all data saved to the SD - the malware developers had simply chosen to target Viber users specifically.

So What Happened?

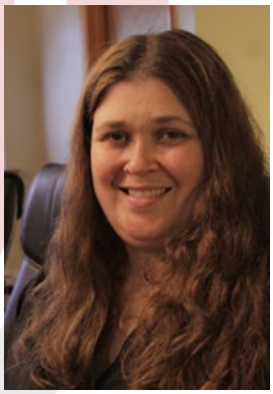
However, there's an excellent case to be made that the app should never have reached the Google Play storefront at all, and that Google's review process seems to need some work.

Upon opening the app, you are brought to the game's main menu screen, with the following options: Help, Players, Statistics, and the all-important New Gane. Yes, you read that right. New Gane. There was a spelling mistake, right there on the most important element of the main menu, visible from the download screen itself, that Google either missed or...

Read the Rest Online!
http://dti.io/unsafeapp

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

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