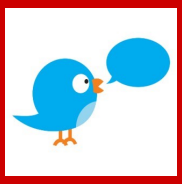
TECHMinutes

November 2016

Your Small Business Technology Information Source!

This Issue:

AOL CEO Gets His Twitter Account Hacked and the Internet Responds Appropriately



Imagine that you are the CEO of a mass media organization whose Twitter has just been hacked and was now posting 20 spam-filled tweets every second. You've just put yourselves in the shoes of Tim Armstrong, CEO of now-Verizon-subsidiary AOL....

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

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

3 Benefits of Managed IT that Every SMB Can Get Behind

Have you ever taken a broken-down workstation or server unit to a break-fix IT technician, only to have them resolve the problem and demolish your IT budget with absurd costs? For small businesses that can't afford to hire an on-site IT department, this is a common occurrence. Thankfully, the SMB now has more options than ever before for how they want their IT to be managed, and it all starts with managed IT services.

The traditional break-fix IT service model might have been necessary once upon a time, but these days, it's beaten out by the efficiency and flexibility that managed IT services can provide.

So What Really IS Managed IT?

The core difference between managed IT versus the traditional break/fix method is that those who are managing the network (namely, the IT company) are treating it as if it was their own. By utilizing enterprise-level remote monitoring tools, carefully honed-in processes, and preventative maintenance, technicians are able to care for the network better. This improves the integrity of the network and all of the devices on it overall, while also identifying problems early before they cause a serious issue. With these tools at hand, caring for your network becomes incredibly efficient, and delivers a level of service far beyond what break/fix IT could provide.

Here are three reasons why managed IT services are the superior choice for your business's technology maintenance needs.

Fewer Unexpected Costs

The average break-fix tech support is expensive, precisely because users can contact them whenever they need assistance. You can think of it as a convenience charge, in much the

(Continued on page 3)

Implementing Softphones for Remote Workers isn't a Hard Decision

One of the biggest concerns that business owners have with remote workers is being able to control and centralize communication. A worker in the office can be plugged right into the company phone system, but how does this translate to those who work from home some or all of the time?

To accommodate these concerns, there is an option to consider. When trying to equip a remote worker with the tools they will need to remain productive and collaborate with the rest of the team, try a softphone solution on a VoIP system.

To translate this tech jargon, a softphone is a phone that functions through software on a computer, using either the conventional phone line or Voice over Internet Protocol to transmit the conversation between the involved parties. Softphones, unlike many exclusively VoIP-based phones, do not require a physical device, and instead reside on any computing solution with an Internet connection. They often include a digitally-based number pad as a part of the program. Therefore, it makes more sense to utilize softphones when

(Continued on page 2)

5 Best Practices to Protect Your Business From Ransomware

Ransomware is an online threat that continues to develop and evolve to accommodate the motives of cyber criminals around the world. Ransomware locks down your business's files and demands a decryption key for their safe return, which makes it difficult (or impossible) to move forward with operations. How can you prevent ransomware from destroying your business's chances of survival?

We'll go over some major best practices to keep in mind when protecting your business from the likes of both ransomware, and other cyber attacks.

- **Have a backup solution put into place:** If your business falls victim to ransomware, chances are that the only shot you have of getting your data back, without paying the ransom, is to restore a recent backup of your infrastructure. More often than not, even seasoned technology professionals can't crack the decryption key, so restoring a backup is the most reliable way of retrieving your data following a ransomware attack (after the threat has been eliminated, of course).
- **Set a schedule for regular backups:** You want your business's backup and disaster recovery solution to restore data to as recent a point as possible. In fact, Directive's Backup and Disaster Recovery (BDR) device is capable of taking snapshots of your data as often as every fifteen minutes. This is necessary if you want to minimize data loss in the face of a data recovery process.
- **Educate your employees about phishing scams:** Another key component of preventing ransomware infections is educating your team about how they spread: phishing scams. Hackers hope that victims of phishing scams will download infected attachments or click on infected links, installing the ransomware. Be sure that your employees know what to look for in a phishing attack, like phony email domains, spelling errors, and other sketchy signals.
- **Update your software solutions regularly:** Those who update their systems consistently with the latest patches and security updates are the least likely to experience hacking attacks. This also extends to ransomware; if you have solutions that are optimized for security, you can prevent phishing attacks from making their way to your inbox in the first place. It's also a best practice to ensure that your systems are as secure as possible.
- **Keep corporate data separate from personal data:** Do you know how data is stored on both your in-house workstations, and your employees' mobile devices? Chances are that if they use laptops or smartphones to perform work remotely, their devices have a combination of personal and corporate data. You should stress that employees keep these two types of information as separate as possible. One way to do this is by storing corporate data in a cloud environment, so that employees don't have to store it on their mobile devices at all.

As always, the best way to protect your business's assets is to prevent ransomware from striking in the first place. Taking the time to prepare your business's infrastructure and train your workforce how to deal with ransomware is the most effective way to keep ransomware as far away from your network as possible. Again, once ransomware has infected your systems, it's next to impossible to remove through traditional means, and will require that you restore the latest backup of your organization's data.

For more information about security solutions or backup and disaster recovery, reach out to Directive at 607.433.2200.

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

Implementing Softphones for Remote Workers isn't a Hard Decision

(Continued from page 1)

equipping your remote worker to remain connected.

After all, as an economic business owner, financing new equipment is always a major consideration before implementing any decision, especially one that revolves around technology solutions. With a good VoIP solution, you can use traditional handsets like you have been used to, but you can also send and receive calls from any smartphone, tablet, laptop, or desktop.

Softphones definitely have the edge when it comes to mobility, as the worker can simply install the client to an existing mobile device and utilize an Internet connection to place or take calls. Also in favor of the softphone is their price, or lack thereof. Without the need for any specialized equipment, a softphone client can be downloaded and set to your device relatively easily. Depending on your plan, there may be costs per user, or costs per device. Therefore, you'll want your IT provider to lay all of this out for you before you make the investment.

Since remote workers need a quick and easy solution they can access on-the-go, softphone mobile clients seem to be the best fit--but that is entirely dependent on your unique situation.

For assistance and advice while setting up your communication solutions, reach out to us at 607.433.2200.

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

3 Benefits of Managed IT that Every SMB Can Get Behind

(Continued from page 1)

same way that you'd get if you went to a restaurant for dinner and tip the waiter or waitress, rather than cook your own dinner. The thing about break-fix IT is that businesses that adhere to that type of model don't care that your technology is broken; they only care about how much money they can make off of your broken technology.

Managed IT, on the other hand, provides users with easily-budgetable payments that are designed to provide the quality tech support needed to prevent major problems from happening in the first place. This means that you're spending less on hardware and software replacements, and you're wasting less capital on downtime that could have easily been prevented. Unlike break-fix IT, managed IT services want to save you money and form a working relationship with your business.

Improved Security and Efficiency

Efficiency is a major pain point for businesses when it comes to IT. Network monitoring and maintenance is required if organizations want to maximize the security of their systems. Patches also need to be administered to all commonly-used applications, but this task is easier said than done. A small business with limited time and resources might forsake them altogether because they're not immediately "necessary." The problem with this lies in security, as unpatched vulnerabilities could allow online threats easy access to your critical systems.

This process is made much easier with managed IT services. Our dedicated technicians can monitor and maintain your systems for critical failures or vulnerabilities, and then resolve them remotely to save you the trouble of the on-site visit. Most issues can be resolved remotely, but sometimes an on-site visit cannot be avoided. However, rest assured that your systems are being watched by the good guys who want to save you money.

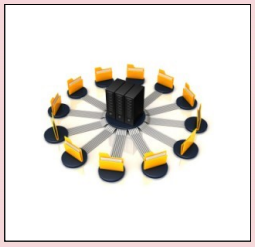
End-to-End Support

On the other hand, some businesses have an internal IT department, but they're either too busy to implement new solutions, or to provide mission-critical updates to systems. Some even have no time to respond to in-house requests for technical support. This can become a major problem that leads to ignored calls for help, decreased… productivity, and in some extreme circumstances, downtime.

However, managed IT seeks to keep your business connected to the support it needs to run properly. Our technicians are just a phone call away. If your…

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

On-Site Backup vs. Cloud-Based Backup, Which is Better?



There's no doubting that data backup is a critical component of any small and medium-sized business's infrastructure. Backup and disaster recovery is important in the event that your organization experiences a death-blow in the form of a data loss disaster. Yet, there's some debate as to whether an on-site data backup solution can be as effective as the cloud. The verdict: both are essential.

According to a survey conducted by research firm Clutch, 46 percent of respondents claim that on-site backup is just as important as cloud-based backup. In comparison, 42 percent of respondents actually prefer on-site backups, while only a meager 11 percent claimed that on-site backup was less important than the cloud-based alternative. The survey asked businesses with up to 500 employees to discover which type of backup and disaster recovery solution they preferred to use.

While it's certainly true that you don't want to exclusively store your data backups on-site, it's important to see the benefits that this can provide. What would happen if your data from the cloud were to be inaccessible for some reason? What if there were complications with deploying your backup from the cloud, like if your backup was too large to migrate back to your network in a reasonable amount of time? That being said, the more locations that your data backups are stored in, the better, as it gives you a better chance of recovering should you be unfortunate enough to face down a hardware failure, flood, electrical storm, or cyber attack.

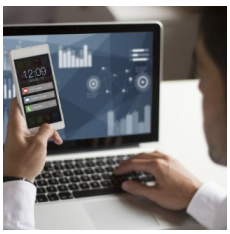
Directive recommends that your business consider the benefits of using a compound backup and disaster recovery solution, one that keeps both an on-site backup and a cloud-based backup for access when you need it most. In particular, our Backup and Disaster Recovery (BDR) solution is capable of providing your business with powerful data backup solutions that practically ensure the survival of your business's critical assets in the event of a disaster.

Our BDR solution can take multiple backups of your data throughout the workday, up to every fifteen minutes. This keeps data loss to a minimum and ensures that your backups will be as recent as possible. These data backups are taken automatically, which eliminates the need for manual execution and clears the possibility of user error. The BDR then sends your data backups to multiple locations, which can include on-site, the cloud, and a secure, off-site data center.

Perhaps the most valuable asset that our BDR solution provides is the ability to...

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

A Step-By-Step Guide to Customize Your Windows 10 Notifications



Windows 10's updates have provided users with entirely new ways to receive notifications, including the ability to sync their notifications via Android's Cortana app. However, you'll be happy to hear that you can control how these notifications appear. We'll walk you through some basic steps on how to customize your Windows 10 notifications.

On the Lock Screen

Notifications will appear on your Windows 10 lock screen, which is great for when you don't want to log into your device, but a privacy concern otherwise. If you want to remove all notifications from the lock screen, go to **Settings > System > Notifications & actions > Notifications**. Then, turn off the switch for Show notifications on the lock screen. Or, if you'd rather just hide certain notifications from appearing on the lock screen, go through **System > Notifications & actions > Get notifications** from these senders.

Select the app that you want to change and select On under the Keep notifications private on the lock screen option.

Set Priority Notifications

You're a busy person, so you understand that not all app notifications should have priority. Thankfully with Windows 10, you can set certain apps to different priority levels to better manage how you receive their notifications. To do so, go to **Settings > System > Notifications & actions > Get notifications from these senders**. Select the app that you want to configure and, under Priority of notifications in the action center, assign it a priority level. You can choose from Top, High, or Normal.

Additionally, you can choose how many of an app's notifications will appear in the action center at any given time. The default is set to three, but you can have it go all the way up to 20. You can change this setting under Number of notifications visible in action center.

Change the Sounds of Your Notifications

You can remove and change the sounds that your notifications make, and it's as easy as going to **Settings > System > Notifications & actions > Get notifications from these senders > Your Chosen App > Play a sound when a notification arrives.** Next, right-click the Start button and open up the Control Panel. Select Sound, which will open up a menu. In the Program Events box, scroll down to Notification and select it. Underneath the Sounds dropdown, you can change the sound that you want to play for your notifications; or, select None to turn them all off.

Turn Off Notifications

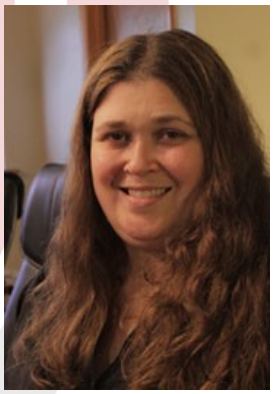
If you're not a fan of notifications, you can turn all of them off, or just those of a select few. Go through **Settings > System > Notifications & actions > Notifications > Get notifications from apps and other senders**. You can then select the apps that you want to receive notifications from under: Get Notifications from These Senders.

For more great tips and tricks, reach out to us at 607.433.2200, and don't forget to subscribe to our blog.

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

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