TECHMinutes

July 2012

Your Small Business Technology Information Source!

This Issue:

Ransomware Wants You to Pay Up

Ever since the Internet became a household commodity, many viruses and malware have donned a social mask; causing harm to computers and data but doing so by deceiving the user. One form of this is ransomware, a type of malware that locks users out of their computer until they pay a toll.

Viruses, malware, and most other online scams are pretty tricky. Much of the time, in order to be effective. . .

Read the rest Online! http://bit.ly/NgZzLU

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.

Read past newsletters at:
newsletter.directive.com

5 Tips for Saving Money on your IT

Saving a little on your technology can go a long ways, but cutting too many corners can lead to additional problems and expensive downtime. Here are a few ways you can cut costs without creating long term issues.

Don't be Afraid to Replace

Got an older PC that's causing you a lot of issues? Older technology is typically more expensive to run, and after a while, it's cheaper to simply buy a new desktop than it is to continue pouring money into something that always seems broken. It's a great time to buy workstations, and if things are tight you can even buy refurbished desktops to keep costs low.

Enforce Energy Efficiency

If you reduce the amount of energy your technology uses each day, your utility bill from the electric company will decrease as well. Switching to LCD monitors (if you are still using old CRT dinosaurs), and enforcing company-wide policies to turn off monitors or put workstations to sleep at night can make a big difference.

Stop Dealing with Vendors

You hired your employees to work, not sit on the phone with a PC manufacturer because your hard drive crashed. Businesses waste money by paying employees to go around in circles with vendor tech support all the time. IT firms like Directive build relationships with vendors and are able to get things done faster. This means issues get resolved quickly and your employ-

(Continued on page 4)

2 Step Authentication for Gmail

Having strong passwords for your online accounts is very important, but sometimes you may want a little more protection in the event your password gets stolen or someone forces their way through it. If you use Google's Gmail service, you can set up your account, then you will need two forms of authentication to get into your email.

Let's face it. You use your email for everything from social media logins to your bank account. More than anything else, your email is the key to your online identity. If an unscrupulous hacker gains access to your email, they could cause havoc that can last for years. Most users are unaware of the potential losses that can result from an email takeover, your bank account could be stolen, and the assets drained. Since most social media passwords can be reset through email, these hackers could also use your accounts on Facebook, Twitter and other social media sites to target your friends and family with phishing attacks. They will also delete all of your saved email in order to frustrate attempts at tracking them. Given the grievous nature of this threat, we here at Directive encourage everyone to take steps to alleviate this threat. Fortunately, Google has provided a simple method to protect your Gmail account from identity thieves.

(Continued on page 3)

Is it Time to Ditch Windows XP?

Windows XP was released back in October 2001, and still today, many users and businesses still use it every day. Even in 2012, XP's market share is around 27%. Is your business still using Windows XP? How much longer should XP be kept around?

Windows Vista put a bad taste in a lot of people's mouths, so for many, sticking with what worked was much more attractive than stepping into the unknown. Windows 7 vastly improved upon the issues found in Vista, but by then many users were content with keeping their older PCs alive.

Microsoft does their due diligence to ease the world into a new OS; they support older operating systems long after they are replaced and work with hardware manufacturers to make it easy to upgrade to the latest incarnation when users purchase new laptops and PCs. Of course, with stellar IT management and a little luck, PCs can last a lot longer than expected, so users don't always feel the need to upgrade.

There are drawbacks to not upgrading, however. Older operating systems quickly become unsupported by third-party software developers, which means upgrades to the other software you use on a day-to-day basis may not be compatible with your OS. Even though Microsoft will continue to support XP and provide security updates and patches until April 2014, most everybody else has moved on to Windows 7 and are gearing up for Windows 8. In some ways, even Microsoft has ceased support for XP already; Internet Explorer 9 and some other Windows applications are only available for later versions of Windows.

Taking advantage of the features in Windows 7 can vastly improve security and performance for businesses, and grant you access to modern best practices and software solutions to increase productivity and improve the way you do business.

Are you still running XP? Contact us at 607.433.2200 for help devising a smooth upgrade plan that will get your company ready for the future.

Share this Article!
http://bit.ly/NgVpUv

The BYOD Revolution

Today, your employees are more and more technologically empowered. With the consumer electronics market teaming with amazing gadgets and high-end devices, cool tech is no longer reserved for fancy geek toys. With employees bringing in their own smartphones and tablets, mobile security becomes a big concern for small businesses.

BYOD, or Bring Your Own Device, is common in todays workplace and you should embrace it, with good reason. Employees that bring their own devices to work tend to be more productive as they are able to view their schedule and email on their device. With the advantage of being mobile, your employees are then capable of handling business matters even when they are away from their desks. Companies that embrace the BYOD model also tend to see increased employee satisfaction and retention rates.

While there are far reaching benefits to the BYOD model, there are also risks. For one, there are so many different hardware platforms and software running on those platforms, accommodating that kind of diversity can be tricky. Moving access control mechanisms to the network is one way to begin addressing the issue. By doing so, any device can access your network without the need for specific on-device management software. Mobile devices most likely are not going to need access to certain critical areas of your network. Restricting access to such assets as a financial database or the like will help to keep those assets safe. Another factor that is common in Mobile Device Management is the ability to wipe the device in case it becomes lost or stolen. This added security measure will make sure that company data stored on the device can be deleted and kept away from those who are not authorized to view it. This is typically done by policies dished out by an Exchange server.

Mobile devices are becoming increasingly present in todays workforce. While they can improve productivity and employee satisfaction, they are just as vulnerable as your desktop computer to malware and other attacks. However with an appropriate security policy and network controls, your company can reap the benefits of a more productive mobile workforce all the while, safeguarding sensitive company data.

Is your business prepared for BYOD? Give us a call at 607.433.2200 to talk about ways to leverage mobile devices for your business.

Share this Article!
http://bit.ly/NgWT0T

2 Step Authentication for Gmail

(Continued from page 1)

First, let's go into a quick review of information security. There are three "factors of authentication" that a user can use to log into their account. The first, something you know, should be familiar to everyone who has email. This is what the user knows. Usually taking the form of a password, but can also been seen in the form of security questions commonly seen on banking sites.

The second factor is something the user has. This factor has a variety of real-world implementations and can be commonly seen as a USB key, RSA dongle or a simple cell phone. The final factor of authentication is something the user is. These (are also known as biokeys) are things like thumbprints, iris scans, or in extreme cases, DNA. The third factor can be costly to implement and might be a little overkill unless you are trying to hide the secret recipe for Coca-Cola. However, Gmail has made it easy and inexpensive to use the first two to protect the key to your digital life.

The first step is to log into your Google account and browse to the settings page. From there, click on Security. You should see a setting for "Two-Factor authentication." Click Edit to turn this on. You'll need a cell phone for the next few steps that Google will throw at you. Once you've got it all set up, log into your Gmail account, this time also entering the texted code at the next page.

This is all pretty nifty, but what if you don't have a cell phone or text plan? Google can still transmit your code through voice calls on a landline. If you plan on traveling and still using your email, you can print off a set of one-time-use codes from the account security page.

You can also set "Application-Specific Passwords" that allow other applications (like Outlook and mobile email) to access your email. Treat these and your regular passwords like your underwear: change them often, and don't share with others.

A lot of people use Gmail for their personal email, but what about your business email? Contact Directive at 607.433.2200 and talk to us about ways to secure your business and prevent crippling attacks from happening to your company.

Share this Article!
http://bit.ly/NgUqU4

Solid State vs Hard Disk

There comes a time when you are looking at a new laptop and you are asked the question: Do you want a Solid State Drive, or a traditional Hard Disk Drive? Well here is a quick run-down of both technologies in the hopes of shedding some light on the issue. By the time you are done reading this article, you will be better able to answer that question.

What is a Hard Disk Drive (HDD)?
A Hard disk drive is a magnetic storage device with several rotating disks (called Platters) covered in a magnetic material on which data can be written. The data is written with Magnetic heads called Read/Write Heads which hover very close to the surface of the platters and, as the name implies, reads or writes the magnetic data on the disk. HDD's are classified as non-volatile storage devices that, unlike RAM memory, continue to store their data after power is turned off to the device. Hard drives are the primary storage device for the users' data and have been since the 1960's

Pros:
Magnetic storage can be written to exponentially more times than solid state

Data can be overwritten directly on the disk

The cost per gigabyte is significantly less than solid state

Cons:
The moving parts inside a Hard Disk Drive provide several disadvantages

While each sector can be written to more than solid state, mechanical failure of the drive will occur before the sector will fail

Because of the moving parts inside, if you drop a hard disk drive, you run the risk of damaging the components. This is especially true if the drive is spinning when its dropped.

Compared to Solid State, Hard Drives have slower read/write speeds and latencies. In fact, traditional hard drives are the bottleneck of modern computing. Where every other component of a PC has vastly improved in speed, hard drives haven't seen much of an increase over the past few years.

What is a Solid State Drive (SSD)?
One of the primary characteristics of a solid state drive is that there are no moving parts. Data is stored in integrat-

(Continued on page 4)

5 Tips for Saving Money on your IT

(Continued from page 1)
ees don't need to deal with less-than-helpful support.

Stop Paying your Phone Bill
Yes, you heard us right. Cease paying your phone company by switching over to a VoIP solution instead. Small businesses save up to 80% on their telephone communication expenses, so the investment pays for itself quickly.

Many VoIP systems allow your users to take their phone and use it anywhere, giving you increased flexibility and functionality.

Get Proactive Monitoring and Maintenance
Nearly all day-to-day IT issues can be completely prevented with just a little bit of maintenance. Directive offers these services to our clients, reducing the amount of downtime they experience. Traditional computer support only fix computer issues when they arise. Directive provides proactive monitoring and maintenance to ensure fewer issues plague your business.

Share this Article!
http://bit.ly/NgTT4x

???? NEED HELP ????

Live Chat Support is available for all your account, technical support or billing questions or concerns.

To use the service go to www.directive.com and click the Live Chat Support link at the top of the page.

Solid State vs Hard Disk

(Continued from page 3)
ed circuits and provide fast access to the stored data. If you have a USB drive, then you are already familiar with solid state drives. SSD's are also non-volatile storage.

Pros:
Solid state drives are not as susceptible to physical shock (like hitting a hard surface) as a hard disk drive.

Solid state provides for faster access to data.

Fragmentation is not an issue on a solid state drive

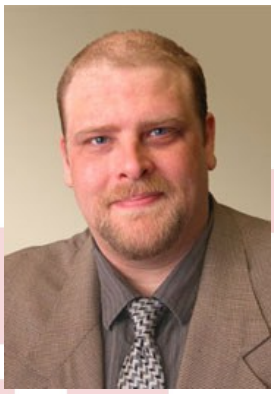
Cons:
Solid state will cost you more per gigabyte than a traditional hard drive.
Each block of memory on a solid state drive can only be written to so many times

Solid state drives have drawbacks regarding data encryption that may leave your data accessible to someone with the right tools.

It is predicted that traditional hard disk drives will co-exist with solid state drives for many years to come and while many of the pros and cons will remain the same, the gap will continue to narrow and solid state drives will eventually become the standard. Even compared to a couple years ago, the cost and longevity of solid state drives has improved. Eventually, it is likely that solid state will take over, but for now it all depends on your needs.

So which one is right for you? That will depend on your needs and budget. While each type of drive has advantages and disadvantages, there are times when one will outperform the other. If your not sure which one to choose, give us a call at 607.433.2200.

Share this Article!
http://bit.ly/NgYzr7



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

facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
newsletter@directive.com