Total Networks
Business IT Done Right

NetworkNews
September 2014

This Issue:

Computing Giants Microsoft and Apple Still Fighting in New Mobile Frontier

Microsoft and Apple have been at the forefront of personal computing since the 1970s. The competition has caused partnerships and strain between the two companies and in the interim, created hardware and software that would change the world. Although the two companies will be forever linked, they both are betting on mobile, and for good reason.

Read the Rest Online!
http://bit.ly/1AaDwxl

About Total Networks

Building on the tradition of providing industry best solutions, the Kinseys continue to invest in tools, training, recruiting, and procedures, continuing to extend our reputation as the premier IT service provider in Arizona.

Visit us **online** at:
totalnetworks.com

Introducing FirmShare℠ by Total Networks - Business Grade File Sync

We live in a world where information equals power.

With the influx of consumer-grade online file-sharing solutions (such as Dropbox, Google Drive, or OneDrive) and Bring-your-own-device (BYOD), distributing information has become easier than ever. As a result, it is now easier for corporate information to fall into the wrong hands intentionally or unintentionally.

With over 200 million users, Dropbox has become the predominant leader for mobile file access. Unfortunately, what works for family pictures does not work with corporate files. In most cases, consumer-grade file sharing services present unacceptable security, legal and business risks in a business environment.

Dropbox poses many challenges to businesses that care about control and visibility over company data. Allowing employees to utilize Dropbox can lead to massive data leaks and security breaches.

Many companies have formal policies or discourage employees from using their own accounts. But while blacklisting Dropbox may curtail the security risks in the short term, employees will ultimately find ways to get around company firewalls.

The best way for businesses to handle this is to deploy a company-approved application that will allow IT to control the data, yet grants employees the access and functionality they feel they need to be productive.

(Continued on page 3)

When it Rains, it Pours - Keep Your Cloud-Based Data Safe

Do you see those black clouds culminating on the horizon? They represent the possibility that hackers will gain access to your cloud storage. Though it is protected a number of ways, it will not stop an experienced hacker. To them, your defenses are as transparent as those thin, wispy, cirrus clouds that are so welcome on a boiling hot summer day.

When it comes to cloud storage security, there are a number of things that you should keep in mind:

Use Obscure Words or Phrases for Your Password

Cloud storage starts with a password, but sometimes, hackers can find ways around them. This doesn't mean that passwords are not safe, but it does mean that the possibility is there, and cannot be ignored. Hackers commonly use brute force tactics, where they attempt to crack the code by randomly inputting passwords. Though this process could take a long time, some hackers are likely more tenacious than you think, and won't give up so easily if they truly want your data. Make sure that your password utilizes lower-case and upper-case letters, as well as numbers and symbols.

(Continued on page 2)

Use a Firewall Before You Get Burned

Too many people think that their systems are safe from the corruption of hackers and viruses. They're wrong. In order to keep your business safe from all of the common threats found on the Internet, you should think about installing some protective software.

One of the most useful types of protection is a firewall. The term originally referred to a wall built to confine a fire within a building, but in this case, a firewall is a type of software that keeps your company safe from the dangers found on the Internet. Believe us when we say that a little protection can go a long way.

What Does a Firewall Do?

When data flows in and out of a network, the firewall is the software that analyzes it. It acts like a bouncer, in a sense. It keeps anything that could damage your computer out of it. Basically, it's a barrier between your network and data that is deemed unsafe and insecure. These threats will most likely be found while surfing the Internet.

> ***"When data flows in and out of a network, the firewall is the software that analyzes it. It acts like a bouncer, in a sense. It keeps anything that could damage your computer out of it. Basically it's a barrier between your network and data that is deemed unsafe"***

Like any barrier, there are many different types of firewalls that vary in strength. These barriers can investigate network traffic, validate connection and data packets, check for legitimate application data, and perform cavity searches on all messages going to and from your network. They are updated regularly to battle against the latest threats, but they're certainly not immortal.

What Doesn't a Firewall Do?

The firewall is definitely a good bet to stop some dangerous activity, but it doesn't solve all of your Internet problems. It's important to understand what you're vulnerable to, even with a firewall, so you know what to avoid and how to deal with threats. Viruses, spyware, adware, and phishing scams are examples of malicious software that bypass the protection offered by firewalls. In addition, firewalls also fail to protect you from infected email attachments or block spam, which can be counterproductive and annoying.

What are my Options?

One of the best security options we can

(Continued on page 4)

When it Rains, it Pours - Keep Your Cloud-Based Data Safe

(Continued from page 1)

Another way to protect your data is to use less-common words for your password, or make up your own, rather than use a common word. Doing so puts you at risk of a dictionary attack, which involves a hacker inputting common passwords. Think about the amount of people who use the word "password" to keep their data safe. Their data isn't so safe if the hacker assumes that they chose an obvious word for their password. Instead, opt for strange or obscure phrases. For example, "D3epSeaRh1n0F1shing#$9? will have hackers guessing for ages.

The Road Less Traveled Sure Has a Lot of Data!

Contrary to what some may think, data can be captured while it's on its way to your cloud storage. While many storage clouds will encrypt the data while it is traveling, you still want to be wary and avoid web applications that do not have "https" in front of the URL. The "s" informs the user that the text's data is a secure, encrypted protocol, and therefore, safe.

Hackers are Lazy

They might work pretty hard to get to your data, but in reality, hackers will likely utilize the easiest means possible to retrieve said data. This generally involves attacking the cloud storage itself rather than your personal data. This can mean that the hacker may not even care about your data and leave it alone, but do you want to take that risk? It's best to use a cloud storage well known for having superior security.

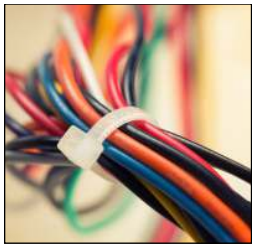
Lock Your Password Away and Swallow the Key

Figuratively, not literally. Keep your password to yourself, and never tell it to anyone. Some hackers will try to get you to fork over your valuable information themselves by claiming to be a service provider, but don't be fooled.

If you aren't sure if you want to trust an unknown cloud source with your precious data, give Total Networks a call at (602)412-5025. We can provide your business with a secure cloud storage solution to fit your company's needs, and we'll do our utmost to ensure that you don't muddle through the oncoming storm alone.

Share this Article!
http://bit.ly/1AaDBBl

Troubleshoot Performance Issues with These 3 Network Cabling Tips



When you experience an error or a performance issue with your company's computer system, you will troubleshoot the problem in hopes of resolving it quickly. Before you open the case of your hardware and start messing with components, check your cables. Even a small cabling issue can cause big problems with your entire network.

Setting up your network and installing cables properly is a surprisingly-delicate procedure that requires a plan called "cable mapping." It's vital that your cables are properly handled. If a cable is defective due to a lack of planning, then it can hinder productivity and even cause downtime. The next time you encounter a networking issue, try out these three cabling tips.

Clean Your Connectors

Remember the old video game cartridges from Nintendo? If you inserted it into the game console and it didn't work, what did you do? You would remove it and blow on it like it was some kind of ocarina (of time). Why did you do this? Gamers implemented this best practice because they thought blowing on the game would remove the dust from the cartridge's connectors and provide a working signal. Often times, this troubleshooting practice would work like a charm and you'd be saving the Mushroom Kingdom again in no time!

> ***"When cables are improperly handled and installed, they bunch up, become twisted, and get pinched. You may be thinking, 'No big deal,' but the reality of cable management is that even a small bend, what's known as a cable microbend, can disrupt the flow of data and cause performance issues"***

In the same way, a dirty cable connector end face can be the cause of performance issues across your system. In fact, this is the surprising top cause of network issues. Resolving an issue can be as easy as blowing on your cable ends. However, for maximum cable cleaning, Processor magazine recommends digging deeper:

Use a simple handheld microscope to inspect the end face. If you detect contamination, there are several good fiber optic cleaning products that can quickly remove the contamination and return the connector to a clean/usable state.

Check for Microbends

When cables are improperly handled and installed, they bunch up, become twisted, and get pinched. You may be thinking, "No big deal," but the reality of cable management is that even a small bend, what's known as a cable microbend, can disrupt the flow of data and

(Continued on page 4)

Introducing FirmShare℠ by Total Networks - Business Grade File Sync

(Continued from page 1)

FirmShare℠ by Total Networks, the most advanced file-based cloud-synchronization platform for businesses, is the solution.

FirmShare℠ by Total Networks provides file sync between PCs and mobile devices. FirmShare℠ enables business users to sync sensitive corporate files between laptops, desktops, smartphones, tablets, and the web. FirmShare℠ makes it possible for users to access all of their files on any device and to collaborate with colleagues, clients, and business partners.

FirmShare℠ unleashes the power of mobility and maximizes the BYOD trend. Despite a diverse computing environment, FirmShare℠ lets users be productive with their files, while giving essential control and visibility to administrators and business owners.

Unlike most consumer-grade file sync services, such as DropBox, FirmShare℠ keeps business files safe by arming administrators with robust security and control features. Organizations can limit or control which devices are permitted to sync; completely audit file syncs and changes; remotely wipe data from devices that are lost or stolen; and monitor and manage how employees are using their mobile devices.

Benefits of using FirmShare℠:

- Managed by Total Networks
- All activity is logged and is easy to track
- Remote wipes of devices when employees leave your company
- Ultra-strong Encryption & 2-factor authentication
- File Server Enablement (Cloud enable your file server)
- Continuous, real-time backup, multiple folder backup, revised file backup
- Granular user-access and security controls

If you would like more information on FirmShare℠, please call us at (602)412-5025, or email sales@totalnetworks.com.

Share this Article!
http://bit.ly/1yrekA4

Troubleshoot Performance Issues with These 3 Network Cabling Tips

(Continued from page 3)
cause performance issues. The best way to avoid such twists and bends is to plan out your network's cable layout so that all of your wires are as straight as possible.

Measure the Power Levels

Your networking cables are able to move data with the assistance of electricity. If the power levels are abnormal, then the flow of data will be hindered. Therefore, being aware of your cable's power levels will be of great assistance in helping you identify which cables are underperforming and should be replaced. To check the power levels of your cables, you will need a simple power meter. Use the meter to measure the power levels at your different connection points, and make a note of the weaker connections. Try replacing the weaker cables with new ones and see if there's a performance boost.

A good IT technician, such as those here at Total Networks, are familiar with other tools that can judge the quality of your Cat5 cables. Your traditional cables contain multiple wires, and if just one is broken, the cable would need to be replaced.

If these simple cable troubleshooting tips don't fix your system's problem, then the issue may be with a hardware component. There are several other troubleshooting measures you can take to try to remedy a networking problem before you do something drastic, like replace a switch.

Total Networks can walk you through tips like these when you call us at (602)412-5025 about IT issues that you may be having. We think the best way to troubleshoot is to first try to do as much as we can remotely with our remote monitoring and maintenance tool. This way, we can save you money by not sending a technician to visit your office unless it's absolutely necessary.

Call us today to save money with your IT expenses. You will be surprised by how easy it is!

Share this Article!
http://bit.ly/1uKpdwv

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email skinsey@totalnetworks.com

Dave and Stephanie Kinsey
Owners

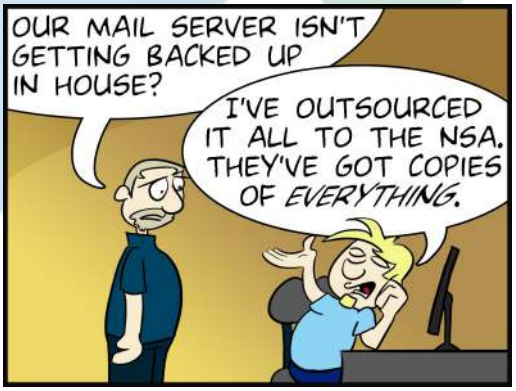
Use a Firewall Before You Get Burned

(Continued from page 2)
provide your company with is called a Unified Threat Manager (UTM) from Total Networks. The UTM is a combination of a strong firewall and other powerful security tools designed to provide protection for your entire network. Most firewalls that initially come with a PC offer so little protection that it might as well be unprotected, but the UTM is a whole different monster.

UTMs vary in shape and size depending on your company's needs, network size, and network traffic. Total Networks can outfit your system with the perfect UTM for your business. We can even provide your company with a free network security audit to patch up the holes in your current firewall. Total Networks can be your own personal firefighter, putting a stop to the catastrophic digital fires that threaten your company.

Share this Article!
http://bit.ly/Xf0GEW

Bill Fox
VP, Customer Service



Total Networks

4201 North 24th Street
Suite 230
Phoenix, AZ 85016
Voice: 602-412-5025

Visit us **online** at:
totalnetworks.com

info@totalnetworks.com
facebook.totalnetworks.com
linkedin.totalnetworks.com
twitter.totalnetworks.com