TotalTechCare
TOTAL TECHNOLOGY SUPPORT

TECHMinutes

October 2016

Your Small Business Technology Information Source!

This Issue:

According to Hackers, Windows 10 Security Passes the Test

Windows is perhaps the most common workplace computing tool, and hackers have been trying for decades to uncover holes in its security. In some cases, like with unsupported operating systems, they've succeeded. However, Microsoft's latest addition to their OS family, Windows 10, seems...

Read the Rest Online!
http://bit.ly/2cnq9ZJ

About Total Tech Care

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:
totaltechcare.com

Don't Have an IT Plan for Your Business? Here are You're a Options

Fact: if the technologies an organization depend on become unreliable, then widespread problems and losses in productivity persist. Therefore, it's crucial for every modern business to have some kind of IT support plan in place. What's your IT plan look like?

There are multiple approaches to IT support available for the modern business. While each approach is inherently different, they all achieve the same thing: providing professional IT assistance. Choosing the right IT support plan is dependant upon your company's IT needs and budget. To help you make the right choice, consider these three options.

Having an In-House IT Department
Having an in-house IT staff is a most-efficient way for businesses to cover their IT needs. However, hiring and retaining IT staff can be a costly endeavor that may be out of reach for smaller companies. Meanwhile, for companies that can afford their own IT department, they can run the risk of overloading the schedules of their IT staff with time-consuming maintenance tasks.

All-too-common situations like this will often force technicians to forgo implementing new, money-saving IT initiatives for the sake of keeping the current systems running. Therefore, IT departments that are feeling this productivity pinch will want to consider supplementing

(Continued on page 3)

Alert: Smartphones Getting Bombarded By Ransomware

Ransomware is as unpleasant a malware as they come, and can ruin your day by encrypting your files until a ransom is paid. Unfortunately, the threat is getting worse, seeing as it's now capable of infecting smartphones, too.

Mobile-based ransomware has been on the rise this year, so much that its presence has nearly quadrupled. Software security group Kaspersky Lab claims that their customers in Germany were victimized by mobile ransomware at the highest rate worldwide. Canada, the United Kingdom, and the United States followed closely. Kaspersky cited that it protected 35,412 mobile users from ransomware between April 2014 and March of 2015. The next year, this total blew up to 136,532 users. These figures include those who were targeted and protected from ransomware hacks, not those that were actually infected with ransomware. That total is likely much, much higher.

Mobile ransomware works in much the same way as it does on desktops and laptops. It infects the victim's phone; however, rather than encrypt files that are stored locally on it (most users have these files backed up anyway), the ransomware will target apps, blocking access to them until the ransom has been paid.

These mobile ransomwares tend to play rough. One example is a ransomware originating in Ukraine that locks the keys and replaces the home screen with a warning from the FBI. The

(Continued on page 2)

Alert: Smartphones Getting Bombarded By Ransomware

(Continued from page 1)

fraudulent warning claims that the user has broken the law by visiting illegal adult-themed websites, and it includes screenshots that incriminate the user. The ransomware demands a $500 fine, paid for with a MoneyPak voucher.

These attacks don't seem to care who they target, either. All you need to do to download it is click the wrong link. In 2014, a 12-year-old girl accidentally installed malware on her device that locked the phone, downloaded repulsive videos, and threatened legal action if she didn't pay the $500 fine.

How can you defend yourself against such a dangerous threat?

Update Your Phone's Software

Malware might constantly be upgrading itself, but so are software updates. This neverending race seems to be in an attempt to thwart the other, and without the most recent versions of each software on your phone, it won't be able to stand up to the most advanced malware on the market. If updated regularly, your device may be able to prevent potential threats from infecting it altogether.

Use Cloud-Based Backup

This is a best practice that should be implemented regardless of whether or not you've been struck with ransomware. In the worst-case scenario, and you have to wipe your device in order to get rid of the ransomware, your files will be safely stored in the cloud, ready to be restored.

Avoid Questionable Downloads

If you can't identify the source of a download, or you simply don't trust it, don't download it. Period. It's as easy as that. Otherwise, you're exposing your device to a potentially malicious entity that could have easily been avoided.

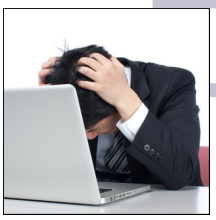
Contact the Authorities

It might seem like a bad thing to do if you suddenly find illegal content on your device, but you need to contact the authorities if you suspect you've been the target of a ransomware plant. In the aforementioned incident with the 12-year-old girl, the authorities were contacted, and they could tell that it was a plant. Even if there is illegal material on your phone, law enforcement members will be able to tell that it's a plant from ransomware.

For more information about how to beat ransomware on any device, reach out to us today.

Share this Article!
http://bit.ly/2cnmGKI

How Employees Troubleshooting Their IT Issues Can Land You in a Dark Place



When it comes to network security, we often see organizations having one of two approaches: 1) They make security a priority by implementing airtight solutions, or 2) They have no clue what network security means. Of course, if a company doesn't have security put into place, employees might take matters into their own hands and implement unauthorized solutions. This is called shadow IT, and it has unfortunate results, even if the user has good intentions.

Shadow IT, also known as the implementation of unauthorized technology solutions of any kind--be it a free antivirus or a substitute for a productivity suite--is known to be a troubling development for security-minded businesses. Basically, an employee might notice a deficit, and take action to resolve it themselves rather than jump through the hoops of dealing with IT.

Or, alternatively, a software license might expire that holds them back from finishing a time-sensitive project. If a user no longer has the tools to accomplish their duties, they'll find a way to do so in order to keep themselves on schedule. Instead of asking IT to handle the problem (especially if IT is flooded with work), the employee will make the decision to use shadow IT, which is a quick fix to their woes, but can lead to other security problems down the road.

Most organizations determine the danger of shadow IT by the source of the downloaded solution. For example, where did your employee find that open-source word processor? Did it come from a reputable website, or did they find it lurking on some message board somewhere deep within the recesses of the Internet? Freeware and open-source software can be helpful when used properly, but more often than not, you'll find that it has installed toolbars on your browser, installed adware, or other threats that could expose your data to external threats.

The problem is that hackers understand that your typical end-user would rather download something free, than pay money for a software license from a reputable vendor like Microsoft. Therefore, you need to address this problem with your employees before it's too late. You should always encourage your employees to approach IT with any concerns about their technology, and educate them on best practices in order to preserve the integrity of your systems. For example, be sure to educate them on how to best use the solutions given to them, as using unfamiliar software is also a major reason why employees might implement shadow IT.

A responsive IT department can go a long way toward keeping your technology infrastructure hiccup-free. When your employees don't have technology difficulties, they can perform their duties more effectively without…

Read the Rest Online!
http://bit.ly/2cno1Bm

Don't Have an IT Plan for Your Business? Here are Your Options

(Continued from page 1)
the workload with co-managed IT services. This is a solution Total Tech Care provides where we come alongside your IT staff and assist them with routine IT maintenance in order to free them up so they can work on bigger IT projects.

Break-Fix IT and Help Desks
Another common approach for SMBs is to rely on an outside IT support system for when something goes wrong with their technology, like a break-fix IT company or a charge-by-the-hour IT Help Desk service. Granted, these are reliable ways to solve IT problems, but they can lead to high IT costs that are impossible to budget around. Plus, the break-fix approach fails to get at the heart of a lot of IT problems, which can often times be easily prevented with a proactive approach to IT maintenance.

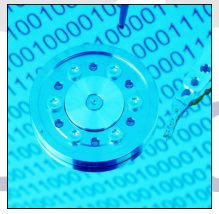
Although, when it comes to IT maintenance, it's inevitable for equipment to break down and for assistance via phone calls to be required. At Total Tech Care, we provide this kind of hands-on support for your broken technology. However, unlike the typical break-fix company which charges for support by the hour, we provide this service at a flat-rate as part of the managed service agreement, meaning that an employee experiencing a technology issue doesn't have to hesitate to contact Total Tech Care for a fix due to the fear of breaking the company budget.

Taking the Proactive Approach With Managed IT
For SMBs looking to gain access to professional IT support that won't break the budget, managed IT service from Total Tech Care is the way to go. Managed IT is a unique offering that's designed to minimize IT issues and downtime by taking a proactive approach to IT maintenance. Plus, thanks to managed IT being offered as a service, it's an expense that you can budget around. This is a great way to make professional IT service affordable, costing you way less than having to onboard new IT staff or pay for a break-fix technician to come and resolve an issue.

When every modern business needs IT support, managed IT puts professional IT support within the reach of every company, no matter the company's size or budget. Have a conversation with Total Tech Care today to learn how managed IT can meet and exceed your company's IT needs!

Share this Article!
http://bit.ly/2crx9ld

3 Features Every Business Needs From Their Data Recovery Solution



As well-prepared as you might believe your business may be against disasters, the reality is that this is not always the case. In truth, you have no idea when you could fall victim to a data loss incident. As a business owner, you need to understand that it's not a question of if you'll experience a data breach, but when, and you need to be prepared for anything.

There are plenty of situations that won't be under your control:

- You aren't going to be able to shield your business's technology from a flood that sweeps through your location and takes half of your infrastructure with it.
- You aren't going to stop your old technology from unexpectedly failing when you need it most.
- An earthquake could knock the ground out from under your business's footing, and with it, your data systems out of commission.
- User error, despite your best efforts to ingrain proper data security practices into your staff, will persist, and could eventually lead to lost data or compromised security.

What can you do to preserve your organization's data?

Data backup and disaster recovery are essential, but the concept is much more refined than it was in the past. Traditional backup solutions used unreliable practices in order to ensure that data was stored and accessible in the event of a disaster. Tape was, and still is, commonly used as a backup measure, in which data is stored on magnetic tape reels that could be deployed when needed.

Now, however, there are much more efficient and less time-consuming ways to take advantage of data backup and disaster recovery, and it's all thanks to the cloud.

Where tape backups are resource-heavy, user-intensive, and time consuming, cloud-based BDR is the opposite. Unlike tape backup that must be performed after-hours, and set by an employee who may or may not forget to do it, BDR is automatic and can be performed throughout the day, all to get past the possibility of an unexpected disaster destroying your data. If you want to guarantee maximum uptime and data retention, you should look for the following features for your disaster recovery solution:

Frequent Backups
Tape backups can usually only be performed once a day, and it's often the case that they have to be done after closing time. Your business needs a solution that can back up your data multiple times a day. Modern BDR solutions can take backups as often as every 15 minutes, so you'll always experience…

Read the Rest Online!
http://bit.ly/2cno28y

3 Expert-Level Search Tips to Help You Find Exactly What You're Looking For

These days, being able to find the exact information you need online is a valuable skill. However, sometimes a website's search capabilities aren't robust enough to be of much use. For this week's tip, we'll show you how to combine a website search feature with your browser's search tool so you can easily find exactly what you're looking for.

To begin, let's go over one of the most valuable tools for online searching, quotation marks. If you need to locate a specific phrase, then enter it into a search engine like Google Search and bookend the phrase with quotation marks. Google will then show you results meeting your criteria exactly, word for word, instead of giving you a bunch of random results pertaining to each individual word of the phrase (which would be the case if you didn't use quotation marks).

While using a major search engine like Google Search to find what you're looking for is one thing, using the search feature of an individual website is completely another. For example, not every website allows you to use quotation marks to narrow down a search within its pages.

If you run into this problem, try instead using the website's search feature to look for one of the two keywords, like "email," and then use your browser's search function to search for a second keyword, "hosting."

To access your browser's search function, simply select **Ctrl+F.** A drop down menu will then appear where you can enter the second word you're looking for. Next, hit **Enter** and the browser will automatically highlight every instance of the second word you're looking for that's located on the open webpage.

When these two searches combine, you'll essentially be able to weed through all the irrelevant search results provided by the website and use your browser to find exactly what it is you're looking for.

Another Way to Search: One way that you can skip having to use a website's search tool altogether (and keep in mind that not every website offers a search tool) is to search the content of an individual website using Google Search.

To do this, type into the Google Search form "site:" followed by the website URL, minus the "http://" and the "www." Following this entry, add what it is you're searching for. So the form should read something like this:

site:website.com email hosting

Add Quotation Marks: To help narrow down your search even further, Google allows you to search individual websites this way and use quotation marks so you can find an exact phrase. For example, **site:website.com "email hosting"** will provide much more specific results than **site:website.com email hosting**.

Ultimately, utilizing Google this way may be more effective than combining the website search and your browser search as previously suggested. Although, you'll still want to keep this double search tip in mind for when you do use a website's search tool and find that it's not working for you. Also, keep in mind that not every website makes its content available to Google Search; using a website's…

Read the Rest Online!
http://bit.ly/2cnpozV

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.

Robert St. Germain
CEO

Tech Fun Fact
The malware used in the Sony hack would have slipped past 90 percent of defenses today.

Total Tech Care

600 W Prospect RD
STE 2G
Oakland Park, Florida 33309
Voice: 866-348-2602

facebook.totaltechcare.com
twitter.com/totaltechcare
newsletter@totaltechcare.com

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