

This Issue:

Start with These Three Questions to See If You're in Over Your Head

Proactive Maintenance Can Save Time and Money

Match Word to Your Style

Do and Don'ts of Managing Your Passwords

BDR Is Better Than Just Data Backup Alone

With Phishing Attacks Beating 2FA, You Need to Be Able to Spot Them

Match Word to Your Style



Microsoft Word's massive cache of options and its relative ease of use are two of its defining

characteristics. This presents organizations and users alike with a large set of different ways they can set up the word processor. Today, we will take you through Word, providing tips on how to change these settings so that you can get the most out of it.

Of course, you will want to consult with your IT administrator before you go to make any major changes.

Customizing Word's Grammar Rules to Meet Your Preferences
There is a good chance that you...



Read the Rest Online!
<https://dti.io/wordstyle>

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

Start with These Three Questions to See If You're in Over Your Head



Technology is a complete necessity these days. It's been proven that, by integrating some technology strategically, businesses can solve major operational problems that many smaller businesses and start-ups can't. Today, we will ask three questions about business tech that any technology-savvy individual should know, and explain why you should know them.

Question #1: Do You Have the Right Technology to Fit your Business' Needs?

This is a question almost anyone that works for your company can answer, but in the grand scheme of things, are you able to efficiently produce your products using the IT you have in place today? If the answer is no, then you absolutely need to consult with one of our technicians.

If the answer is yes, however, you may be surprised about the big benefits that small improvements to your IT can create. If you think your IT is ship-shape and is working optimally for your business, you'll likely be surprised when you discover there are several productivity-enhancing options that you haven't even considered.

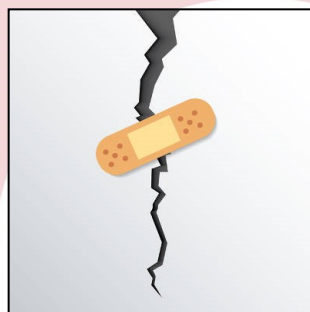
Often, our technicians find that businesses are using antiquated hardware and software, paying too much for their services, or not proactively managing their company's IT, leading to costly downtime and inefficiency. This leads us to our second question:

Question #2: Are Your Servers, Workstations, End Points, Networking, and Security Being Maintained?

You may have a home computer that you don't manage. You turn it on when you need to use it, and you don't worry about how efficiently it is running, until it begins to stall, applications close for no apparent reason, and its overall performance starts to lag. If this were

(Continued on page 2)

Proactive Maintenance Can Save Time and Money



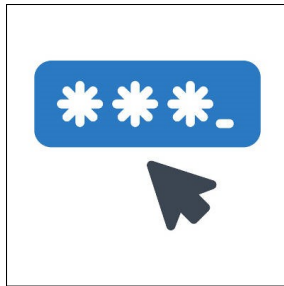
Technology management has always been a problem for small businesses. Whether it's a matter of affording proper technology maintenance or not having enough time in the workday to get around to maintenance, it's likely that your small business has to manage limited resources that make it difficult at best to make preventative maintenance occur. We're here to tell you that there's a better way to get the IT help you need.

Think about the way that businesses went about IT assistance in the past. Finding professional IT resources isn't always your first instinct. In fact, the first thought you might have is that as long as your technology is working, you have nothing to worry about; you'll cross that bridge when you get there. The problem is that technology management and maintenance will always be a problem for your business if you don't take steps toward this goal right from the beginning.

The traditional method of IT maintenance is what we in the industry call "break-fix." Break-fix IT management is when a company seeks out the assistance of IT professionals when their technology fails to operate as intended rather than actively seeking to keep it in

(Continued on page 3)

Do and Don'ts of Managing Your Passwords



Password security is a tricky part of running a business. After all, it's not just dealing with your own pass-

word, but those of the many employees all throughout your organization. In times like this, it's helpful to provide them with a list of how to make the best passwords possible. Here are a couple of examples for what to do, as well as what you shouldn't do, when building a proper password.

Password DOs

Passwords don't have to be difficult.



Here are some easy-to-follow tips for ensuring your passwords are as secure as possible.

- **Use long passwords:** Generally speaking, the longer the password is, the better for security. Of course, the contents of the password still matter, but we'll get to that soon enough. Aim for a length of at least 16 characters.
- **Use special characters, numbers, and symbols:** Simply using letters isn't enough. You should strive to put together a password that consists of both upper and lower-case letters, numbers, and symbols.
- **Use alphanumerics:** You'd be surprised by how much more effective alphanumeric passwords work. Try

replacing an "i" with a "!" or an "a" with an "@" symbol.

- **Try out passphrases:** To bypass the annoyance of remembering passwords, you should use passphrases. These are short phrases that are easy to remember, but difficult to guess. A good example is, "iL0veW@ffle\$2much" instead of "iLoveWafflesTooMuch."
- **Use different passwords for every account:** We know what you're thinking. Remembering more than one complex password is impossible! We know it might seem difficult, but using different passwords is critical to the success of your online accounts. If one is used for multiple accounts, and that account were to be compromised, all others that use that password would also be at...



Read the Rest Online!
<https://dti.io/doanddonts>

Start with These Three Questions to See If You're in Over Your Head

(Continued from page 1)

to happen with your work computer, you'd have a bit of a problem, right? Now think about how people you pay to work for you feel when their workstation starts to go on the fritz. You didn't pay a premium price for that machine, after all.

Expecting someone to excel for your company on computers that don't work properly is like asking a lumberjack to do his job with a steak knife. Sure, it may do the job, but it's going to take a lot longer and a lot more effort and bother to do it than it should. This is why it is crucial to make sure that all of your organization's workstations, servers, and other hardware are properly maintained, and that the software tools you rely on are patched and up to date.

It typically takes a certain degree of experience to gain the practical knowledge needed to do a job proficiently. Managing technology is no different. You have to know when to move away from a certain technology,

when to embrace others, and just about everything about these complex systems in order to keep it maintained well and working for your business. Remember AOL? In retrospect, they should have used their profits to update to broadband. They didn't - which is why we had to ask if you remembered them. Learning which technology to use and when you need to use it can go a long way toward taking your company to where you want it to go. You can do this with knowledge.

Question #3: Do You Have Access to the Knowledge Your Business Needs?

What hardware do you have? What software do you use? How much do you spend on downtime a month? How much do you spend in printing costs? Questions like these are simple ones that shouldn't take you long to answer, but when you can't answer them, or other basic IT questions, you typically find someone that can. At Directive, there is one thing that we have in spades: Knowledge about business technology.

When a business owner comes to see us about their technology, we don't immediately jump into the sales process. The first thing we do is ask questions. Sometimes we do a complete network and infrastructure assessment before we even start to talk about selling anything to you. Our business technology expertise is based on a knowledge of these systems, and finding solutions to problems; and, rest assured, if yours is like many businesses we encounter, you have complications that you've encountered that you don't even consider to be problems.

The difference is that we have the experience and knowledge to provide the value you are looking for from an IT consultant. Call us today at 607.433.2200 to have a conversation that you won't regret, because it may open your eyes to a way forward.



Share this Article!
<https://dti.io/overhead>

Proactive Maintenance Can Save Time and Money

(Continued from page 1)

proper working order. While this might seem like the proper course of action (after all, who wants to pay for services they don't need at the moment?), this creates a dilemma for your company. You might be saving money in the short term, but you're also drastically losing money in the short term whenever you experience technology troubles. In other words, since you're waiting for your technology to break down before addressing issues with it, you're

experiencing downtime that could have been prevented earlier on.

The alternative to break-fix IT--managed IT--is perhaps the greatest way your organization can save money on IT maintenance and management. Managed IT turns the capital expense of maintaining your technology and transforms it into an operational expense. What was a significant hit to your budget at any given time is instead a more manageable monthly payment that can

be stopped or scaled as needed. It's an easy and convenient way to manage your technology.

Directive can help your business get started with managed IT services. To learn more, reach out to us at 607.433.2200.



Share this Article!
<https://dti.io/savemoney>

BDR Is Better Than Just Data Backup Alone



Maintaining a proper data backup system is one of the most important parts of business continuity, even if

it's something you'd rather not think about. If you don't take data backup seriously, your organization is at considerably greater risk compared to what it would be like if you had it. We'll walk you through the proper steps toward making your organization's future more secure through data backup.

Data Backup vs Disaster Recovery: What's the Difference?

Some organizations use data backup and disaster recovery as if they are interchangeable, but the fact of the

matter is that they are two very different things. In reality, data recovery isn't possible without data backup, and vice versa.

Data backup consists of actually creating the record of your data to be restored at a later date, whereas disaster recovery is how and when you restore the data from the data backup. Basically, one of them can't happen without the other, and they are both integral parts of the business continuity process.

Details on Data Backup

Of particular note when considering data backup is what data will need to be focused on in order to ensure minimal operational deficiency during the restoration period. In other words, how much data is acceptable to get back into a situation where your business can operate as intended? A good rule to

practice is to back up enough so that you can get back in action following a disaster with minimal downtime. Remember, the best backup system is one that happens automatically, so think about how the process is being initiated, too. The ideal solution is one that isn't affected by user error.

Details on Disaster Recovery

Disaster recovery is focused primarily on how long it takes for a restoration to occur. In other words, how fast can you get back to a decent state of operations following a disaster so that you're not operating at a loss. A significant part of this process is ensuring that you have access to a data backup in at least three locations: one on-site, one in the cloud, and one located in a secure off-site data center. You should also consider testing your backups regularly to ensure that they will occur without a hitch, meaning that you won't find yourself between a rock and a hard place when your backup system fails in the future.

Directive can help your business implement an all-in-one Backup and Disaster Recovery (BDR) solution, enabling even a small business with a limited budget to maintain a proper data backup system. You'll be prepared for even the worst circumstances. To learn more, reach out to us at 607.433.2200.



Share this Article!
<https://dti.io/betterbdr>



With Phishing Attacks Beating 2FA, You Need to Be Able to Spot Them



Unfortunately, one of the most effective defenses against

phishing attacks has suddenly become a lot less dependable. This means that you and your users must be ready to catch these attempts instead. Here, we'll review a few new attacks that can be included in a phishing attempt, and how you and your users can better identify them for yourselves.

How Has Two-Factor Authentication (2FA) Been Defeated?

There are a few different methods that have been leveraged to bypass the security benefits that 2FA is supposed to provide.

On a very basic level, some phishing attacks have been successful in convincing the user to hand over their credentials and the 2FA code that is generated when a login attempt is made. According to Amnesty International, one group of hackers has been sending out phishing emails that link the recipient to a convincing, yet fake, page to reset their Google password. In some cases, fake emails like this can look very convincing, which makes this scheme that much more effective.

As Amnesty International investigated these attacks, they discovered that the attacks were also leveraging automation to automatically launch Chrome and submit whatever the user entered on their end. This means that the 30-second time limit on 2FA credentials was of no concern.

In November 2018, an application on a third-party app store disguised as an Android battery utility tool was discovered to actually be a means of stealing funds from a user's PayPal account. To do so, this application would alter the device's Accessibility settings to enable the accessibility overlay feature. Once this was in place, the user's clicks could be mimicked, allowing an attacker to send funds to their own PayPal account.

Another means of attack was actually shared publicly by Piotr Duszyński, a Polish security researcher. His method, named Modlishka, creates a reverse proxy that intercepts and records credentials as the user attempts to input them into the impersonated website. Modlishka then sends the credentials to the real website, concealing its theft of the user's credentials. Worse, if the person leveraging Modlishka is present, they can steal 2FA credentials and

quickly leverage them for themselves.

How to Protect Yourself Against 2FA Phishing

First and foremost, while it isn't an impenetrable method, you don't want to pass up on 2FA completely, although some methods of 2FA are becoming much more preferable than others. At the moment, the safest form of 2FA is to utilize hardware tokens with U2F protocol.

Even more importantly, you need your entire team to be able to identify the signs of a phishing attempt. While attacks like these can make it more challenging, a little bit of diligence can assist greatly in preventing them.

When all is said and done, 2FA fishing is just like regular phishing... there's just the extra step of replicating the need for a second authentication factor. Therefore, a few general best practices for avoiding any misleading and malicious website should do.

First of all, you need to double-check and make sure you're actually on the website you wanted to visit...



Read the Rest Online!
<https://dti.io/spotphishing>

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



newsletter@directive.com



facebook.directive.com



linkedin.directive.com



twitter.directive.com



blog.directive.com



instagram.directive.com

Visit us online at:
newsletter.directive.com

