

## This Issue:

Seasons Greetings!

5 Tips to Consider for Your IT Budget

5 Clues that an Email is Really a Phishing Scam

Fight Workplace Distractions With These 3 Tips

The Most Dangerous Threats to Your Business Could Be Internal

3 Vendor Scenarios You Can Do Without

2 Important Networking Trends You Must Consider



On behalf of everyone at Directive, we'd like to thank you for making this such a wonderful year, and we look forward to many more opportunities in the years to come. We truly appreciate you and your business. Sending the warmest of holiday wishes from our family to yours. **Please note that our offices will be closed in observance of the upcoming holidays on December 24th, 25th and 31st. Emergency support will be available for our managed service clients.**

### Fight Workplace Distractions With These 3 Tips



What's your reaction to your mobile device beeping at you? If you're the kind

of person that drops everything to see what it says, then you're probably way more distracted at work than you should be. It's a bad habit to look at your phone every minute or two, but...



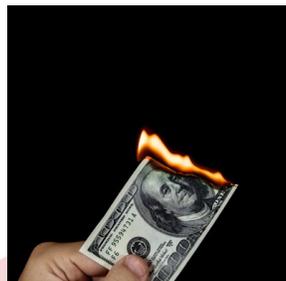
Read the Rest Online!  
<http://bit.ly/1QxZWm6>

## 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](http://newsletter.directive.com)

## 5 Tips to Consider for Your IT Budget



Putting together an IT budget is an exceptionally tricky procedure. Every year presents unique technical challenges that need to be addressed, but the slightest miscalculation can be detrimental to an IT budget. Here are five tips to give your organization some breathing room when it comes to planning out next year's IT expenses.

### Think in the Long Term

When planning out your IT budget, it's important to consider both short-term and long-term investments that you'll be making for the sake of your business. The fact that so many services, like cloud computing, are being turned into operational expenses, is placing an emphasis on a model based around affordable payments rather than heavy up-front costs. It's important to consider how these costs will affect your budget, especially over the long-term.

*(Continued on page 3)*

## 5 Clues that an Email is Really a Phishing Scam



One of the most masterful arts of deception that hackers use is the phishing attack, which attempts to steal sensitive credentials from unwary victims. The anonymity afforded to criminals on the Internet is what makes this possible. Using phishing attacks, hackers attempt to steal credentials or personal records by forging their identities. What's the best way to protect your business from these attacks?

Just like any other kind of fishing trip, a hacker will cast out their line by sending emails disguised as legitimate organizations. They then hope that someone will bite--someone who's willing to provide the requested credentials or information. What a lot of users might not realize is that phishing emails are pretty obvious, if you know what to look for.

*(Continued on page 2)*

## The Most Dangerous Threats to Your Business Could Be Internal



Most of the time, when it comes to cybersecurity, businesses tend to focus primarily on external threats rather

than those that might be lurking in the shadows of their internal operations. Believe it or not, the most dangerous entities out there could very well be working for you, right under your nose.

### What Constitutes an Inside Threat?

While there are a number of entities that can threaten your business, many of them come from within. Included are previous workers who might not have left on the best terms, current employees who could be engaging in corporate espionage, or even unknowing end-users who might have allowed external hackers to compromise your network infrastructure.

- **Irate former employees:** Some employees will quietly pack their things and be on their way without saying a word. Others will make a big fuss and leave in a flurry of rage. It's the

latter that you have to worry about, simply because they could lose their head and leak any information, like passwords and whatnot, to the web. Or, if they're feeling particularly sneaky, they might attempt sabotage themselves.

- **Suspicious co-workers:** If there's some behind-the-scenes action going on in your business, you might suspect that someone internally is behind it. Issues like stealing equipment, devices, or even data, can arise for a variety of reasons. However, it's most likely for personal gain, like monetary compensation or to assist themselves with other endeavors outside of your business.
- **End-user error:** Unlike the previous two examples, workers who have made mistakes and cost the company its data security or worse don't necessarily do so on purpose. This can often be seen by the spear phishing hacker, who will target unsuspecting employees and coerce information out of them with phishing scams.

### How You Can Protect Your Business

In order to ensure that your business

follows a policy that mitigates insider threats, be sure to follow this action plan:

- **Integrate an office security system:** While this might seem like a far-fetched idea, it's a very common occurrence in the small business environment. Organizations just like yours take advantage of security systems to ensure that nobody is breaking into the building, trespassing where they aren't supposed to, or taking part in any sketchy activity.
- **Monitor and maintain your access logs:** If you're concerned that there might be some suspicious activity on your network, you should integrate a comprehensive monitoring solution, complete with access logs that can tell you who accessed the network, from where, and when. This helps to keep only approved users from accessing the network.
- **Perform exit interviews:** When someone leaves your business, you should implement a thorough...



Read the Rest Online!  
<http://bit.ly/1kPwHi0>

## 5 Clues that an Email is Really a Phishing Scam

(Continued from page 1)

### Take a Good Look at the Message's URLs

Many phishing emails try to hide their schemes behind legitimate-looking URLs in the message. Some links will be designed to either direct you to a malicious web page, or execute a download of malicious files. Either way, you don't want to be caught in this situation, so take a moment to hover over the links (don't click them) and check to see where they really go. You should see the real destination appear in the bottom-left corner of your web browser.

### Does the Message Request Personal Information?

The main goal of a phishing scam is often the obtaining of sensitive credentials or personal information. This includes So-

cial Security numbers, credit card information, usernames, passwords, and so much more. Some of the more elaborate phishing scammers will go out of their way to make it look like they're someone you know, be it a local bank representative or government official. It's important to keep in mind that nobody will request your personal information through an email. Large organizations will almost definitely contact you via direct mail before anything else. Never send anyone your sensitive information through email, for any reason.

### Does the Message Look Unprofessional?

While the rules of proper spelling and grammar elude a vast majority of people at times, you can generally count on large companies to practice proper communication etiquette with their emails.

Therefore, if your inbox is filled with emails from, say, Microsoft, and these messages are full of spelling and grammar errors, it's safe to assume that it's not a legitimate email, and you should treat it as a threat.

### What Exactly Are They Talking About?

Some phishing scams will act like you've won a great prize and need to claim it immediately. An example of this is a message claiming that you've won the lottery, and you need to claim the money before it's too late. Think logically here; if you haven't entered to win anything, you shouldn't expect any messages like this. Either way, it's a safe bet that...



Read the Rest Online!  
<http://bit.ly/103CGtx>

## 5 Tips to Consider for Your IT Budget

(Continued from page 1)

### Invest in Training Your Staff

There's far too little investment in ensuring that employees understand the benefits of the latest technology solutions. What good are the latest IT solutions if your staff has no clue how to use them? By properly training your team on how to take advantage of this technology, you're essentially providing them with skills necessary to make their workflow easier and more convenient. This helps them get the most out of their technology and maximize the amount of work they're able to perform. Carefully Consider Storage Options

Your organization shouldn't just be taking advantage of one centralized storage system for its data. Instead, you want to have multiple avenues where your data

can be stored. One of the primary reasons for this is because you need to make sure that your data won't be wiped out in one fell swoop (redundancy is crucial). Another reason for this is to optimize your organization's access to its critical data. For this purpose, cloud computing can be exceptionally helpful, for both data storage and data backup solutions.

### Account for Anticipated Software/Hardware Upgrades

Unexpected hardware failure can be a pain to deal with, especially if your budget hasn't taken these issues into account. Not only are hardware failure and software issues hard to predict, but they're also expensive to replace. Your budget should always have assets allocated toward mitigating and replacing

technology that's critical to the success of your business. Otherwise, you could be dealing with huge expenses that will, without a doubt, break your budget, and force you to come up with funds from elsewhere.

### Take Advantage of Outsourcing and Consulting Services

Outsourcing management responsibilities is typically very budget-friendly, considering you're turning up-front costs into operational expenses that can be paid for over a specific time period. In other words, you can think of it as enjoying all of the benefits of purchasing a brand new solution, without the expensive price tag.



Share this Article!  
<http://bit.ly/1kPtUpb>

## 3 Vendor Scenarios You Can Do Without



Vendors can be a hassle. You need their product or service to keep the gears of business turning, but some-

times, having to deal with vendors can be way too time-consuming. This is where our vendor management service comes in.

With Directive on your side, we can handle all technology vendors for you so that you don't have to. This is what it looks like to have a "single point of contact" for any and all of your technology-related needs. Image not having to deal with these three common technology vendor annoyances.

### Vendor Acquisitions

The speed of business moves rapidly. Sometimes a vendor will go completely out of business, requiring you to find a new supplier. Other times, a vendor might get acquired by another company and your account will get mishandled in the transition. At the end of the day, you don't much care who bought out who

and which company folded up; all you care about is keeping your business supplied with working hardware and supported software.

Instead of having to be bothered by business moves that are outside of your control, let us coordinate your accounts to find you new, trustworthy vendors that best suit your needs.

### Drama with Your Vendor Account Manager

Have you ever dealt with a vendor point of contact that just happens to rub you the wrong way? Maybe they have a poor attitude, or maybe you've had a major disagreement with them in the past over billing. Then there are some companies which seem to have a revolving door when it comes to their point of contact, which means that you've got to explain the particulars of your business to a new account manager way too often than you should have to.

Directive can relieve this vendor drama by working with technology vendors on your behalf. One way that we do this is by taking the time to learn the intricacies of your business and what your

needs are, which effectively makes us a liaison for your company's technology needs.

### When You Experience Problems with Mission-Critical Technology Services

When you experience a problem with a mission-critical technology service like your Internet connection or cloud hosting service, it's on you to drop everything and call the vendor to get the situation resolved. TechRepublic offers this scenario which you may have experienced:

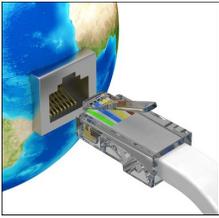
You consign a major system to a cloud-based vendor because the vendor has a reputation for being reliable and best in class—then the vendor has a failure that puts all your users offline and has a dire impact on [your] company's business.

When dealing with nightmare scenarios such as this, you're going to want a professional on the phone representing you. You need someone in your...



Read the Rest Online!  
<http://bit.ly/1kPxkrZ>

## 2 Important Networking Trends You Must Consider



One sometimes-frustrating aspect about

computer networking comes from the always-changing nature of technology. For example, let's say that you have your network perfectly set up with everything running smoothly, then comes along some newfangled IT trend or mission-critical technology workflow that requires you to change everything. You can't prevent this from happening, but you can stay on top of the latest IT trends so that you're not caught off guard.

To that end, here are two IT trends that will cause you to make some major changes to your company's network.

### Mobility (BYOD)

Business today is going mobile as workers utilize their personal devices for work purposes. Many companies are adapting to this trend and providing their staff with mobile devices so they can get work done more efficiently. Providing devices for your staff takes away the worry that's inherent from the security risks of BYOD (bring your

own device). In fact, in a recent IT survey by Forrester Research, "65 percent of respondents said they plan to expand their enterprise mobility services to meet their business priorities."

What this means for your business is that you're going to have to accommodate this trend, or else have your network be overwhelmed by mobile devices. One of the challenges of BYOD is that it opens the door to twice as many access points that all need to be managed and secured. Plus, you're going to need to increase your network's bandwidth, or else experience some major lag issues when the number of mobile devices accessing company files inevitably doubles.

### Unified Communication and Collaboration

What you're sure to run into as you continue to do business in the modern age is more companies and clients requesting meetings via video conferencing and other digital collaboration tools. Network-Computing explains:

Communications and collaboration solutions now allow businesses to assemble the

best people to do a job, regardless of their location. Information sharing between companies – in organizational settings; between suppliers, vendors and clients; or for special projects – has also become the norm.

If your business isn't equipped with these tools, then you're going to miss out on potential sales and networking opportunities, as well as a powerful way to streamline internal communications with your team. Equipping your network with a solution like Voice over Internet Protocol will give you the modern communication capabilities that you need, without crippling your current IT infrastructure. Directive can provide you with a VoIP solution that's perfect for your needs.

Of course, these are only two IT trends that promise to disrupt your company's nice and tidy IT network. Also, be on the lookout for advancements in cloud computing, big data and analytics, new security compliances, and The Internet of Things--they're sure to really shake things up...

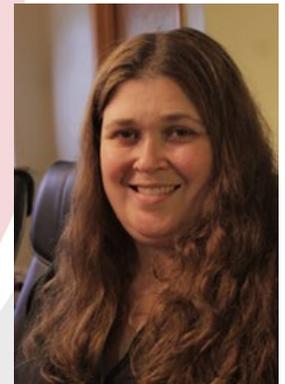


Read the Rest Online!  
<http://bit.ly/1QxXLij>

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](mailto:newsletter@directive.com)



[facebook.directive.com](https://facebook.directive.com)



[linkedin.directive.com](https://linkedin.directive.com)



[twitter.directive.com](https://twitter.directive.com)



[blog.directive.com](https://blog.directive.com)

Visit us **online** at:  
[newsletter.directive.com](https://newsletter.directive.com)

