directive

TECHMinutes

November 2020

Your Small Business Technology Information Source!

This Issue:

4 Cybersecurity Tools You Need to Know About

It may be an understatement to say that business has been difficult thus far in 2020. With all that is going on, nobody should have to deal with cybercrime. Unfortunately, it remains a major consideration for every IT administrator and business owner. With complex solutions being developed to help ward off these cyberthreats, strategies are changing. Today, we thought we'd take a look at four security tools your business should consider to help keep these scammers out of your network...

Read the Rest Online!
https://dti.io/fourtools

"*Be present in all things and thankful for all things*." - Maya Angelou.

Technology Improvements Give Your Businesses a Leg Up

In today's business, technology seems to be advancing at an alarming rate. Just when you think you've got the latest and greatest tech; something is developed that makes your new tool seem antiquated. Nowhere is this more evident than in the management of your IT.

As the tactics have changed over the years, the technology has changed with it. We thought we would outline how the industry has changed over the years and discuss some of the technology used that we use and how we are always trying to improve the ways we streamline the management and support of your business technology.

Project and Support Documentation

For an IT service provider, managing projects is the name of the game, and is typically one of the most difficult parts of the job. For most of the past decade software developers have attempted to create tools for businesses to use that make project management easier. By

(Continued on page 2)

Bad Situations Can Come Down On Your Business Through Phishing

For the past several years, ransomware has been a major thorn in the sides of businesses. Hackers that were once known for "hacking" into networks, changed tactics when encryption just got too strong. Today, these "hackers" use confidence tactics to gain access to accounts. Once they're in, their strongest tool is ransomware. Let's look at what makes ransomware so dangerous and how your company can combat the constant attacks that come your way.

A Brief Look at Ransomware

Being on the receiving end of a ransomware attack is terrifying. First, you log into your computer as usual only to find that files, drives, or even network attached resources are completely inaccessible. What's worse is that staring you in the face is a ticking clock and a message saying that you need to pay a ransom in Bitcoin or else the files, drives, or network resources will be gone forever. It's not a great situation. Many organizations (including entire municipalities) have suffered from this and have been forced to pay the ransom only to get hacked again days or weeks later (we don't recommend you try to negotiate with hackers).

(Continued on page 3)

25+ YEARS IN BUSINESS est. 1993

More Effective for Business: Wireless vs Wired

Businesses' data needs are rapidly changing. Today, data security is a pressing issue. Unfortunately, the amount of dangerous threats are expanding as well and it is important to ensure that any technology moves you make don't end up putting your business in harm's way. This month, we'll talk about the pros and cons of wiring up your computer network.

The Wired Connection

The Pros

The pros of a wired network connection are mostly in the additional speed and reliability you see from hooking wires up. IT administrators have more control over which devices can connect to a network which presents opportunities to maximize your ability to maintain security.

Another benefit of a wired connection is that they are typically faster than wireless networks. The additional speed that your organization could see is improved further if your business has walls, floors, ceiling, and other obstructions that would typically cause more interference with wireless connections.

The Cons

One major problem wired networks have is that they don't always allow for the type of cooperative working relationships that strong and powerful wireless networks deliver. By having all computing resources wired to network switches, intra-office collaboration suffers.

The main problem with a wired strategy is that before you can take advantage of the security benefits and the speed, you'll have to successfully connect everything. Any person that has tried to wire a connection across a busy thoroughfare knows that running cable and hiding wires is a major pain in the neck.

The Wireless Connection

The Pros

Obviously, the major benefit of having a strong wireless network anywhere is that devices that don't offer the option to be wired into the network, like…

Read the Rest Online!
https://dti.io/wirenetwork

Technology Improvements Give Your Businesses a Leg Up

(Continued from page 1)

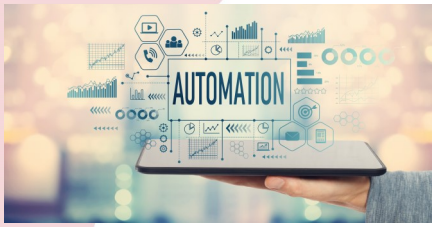
integrating innovative time and task management tools, we can easily set guidelines for success, and keep your team working effectively until a successful conclusion to a project is made.

Much of the innovation has been in the way that we've dedicated to documenting everything. We utilize a slew of tools to manage our everyday support responsibilities, scheduling our technicians, maintaining our communications with you, and keeping track of projects, but without our massive internal library of best practices and documentation, repeat issues would be a real problem.

It goes much further than simply having an archive of all of the problems we've solved though—we document absolutely everything and tie it all together based on the hardware and software in use. Here's a perfect example:

Let's say that a few users on your network report weird slowness issues when accessing certain files on the network. We spend time troubleshooting the issue, and it turns out to be a particular access point. Six months later, it happens again. We're able to look up the history of support for that particular access point and use the data from past support tickets to more rapidly determine a solution or make the decision to swap out the access point.

This makes it so remedies for oddball issues rarely have to be started from scratch, and it's a huge part of keeping things running smoothly. We also thoroughly document model and serial numbers, warranty information, installation info, product keys, and a whole lot more to ensure that your network can be audited at any time and support is as effective as possible.



IT Automation

One of the biggest differences between IT management of the past and today's current IT services environment is the presence of so many automation tools. Larger organizations have benefited from many of these tools for a while now, but for the small and medium-sized business, it has been difficult to consistently manage and maintain hardware and software resources.

With more businesses using multiple tiers of computing: some locally hosted and some cloud-hosted, it is important that there is at least a basic understanding of how these systems interrelate. Today's monitoring and management tools are getting smarter, making it easier for us to automate certain tasks. This ensures that we can not only manage your whole organizations' computing infrastructure remotely but allows us to ensure that any inconsistency is remediated quickly to avoid problems with production. Today's software also provides a level of transparency that wasn't possible only a few short years ago. With data driven insights that provide the information needed for well-informed decisions regarding growth and maintenance to be made, resources can be made available faster, allowing your business' pace to…

Read the Rest Online!
https://dti.io/advanctech

Bad Situations Can Come Down On Your Business Through Phishing

(Continued from page 1)

Phishing

Ransomware doesn't just get onto business networks and into endpoints, it needs help. Phishing is commonly used to assist it. Phishing is a term used to describe a social engineering attack strategy where scammers attempt to use subterfuge and deceit to make people provide access to computing systems and networks via email, instant message, telephone calls, and any other type of commonly used communication.

Cybercriminals have taken to pairing these attacks together to con as many people as they can. If someone on your business' computing network incidentally clicks on a link or unpacks an attachment that looks benign on the surface, but deploys this nefarious code, your business may be in big trouble.

What to Look for in a Phishing Email

There are some warning signs that a message is a phishing attempt. They include:

- **Details are wrong** - There are several details that you should check before you click anything in an email. Is the email address from the sending company? Are there misspellings and grammatical errors that you wouldn't find in professional correspondence? Were you expecting an email from the company? If there are obvious inconsistencies, make sure to report it to your IT administrator before proceeding.
- **There's a lot of urgency** - Most phishing emails have desperate call-to-actions. Email is a useful communication tool, but it is rarely that users are directed to do anything that would necessitate you plugging in any type of sensitive data. If an email's message seems a little…

Read the Rest Online!
https://dti.io/badphish

Solid Backup Helps Builds Continuity

With a lot of business owners being extra cautious about their spending and doing what they can to prevent unexpected interruptions they are doing everything they can to prevent data loss. This month, we thought we would tell you how data redundancy can help towards this goal.

Data loss can happen a few different ways. Malware can cause irreversible data loss. Your end-users can mistakenly cause data loss by overwriting or deleting data. A disgruntled employee could do even more damage by intentionally sabotaging your systems. Think about it this way: your data is stored on mechanical devices that are prone to corruption and mechanical failure when jostled just right. These devices don't last forever and over time, their propensity to fail increases. If your data is only stored in one place, and that drive fails, you lose everything.

Data Loss Hurts in a Lot of Places

It can be a burden on your company when you lose any amount of data. If an entire hard drive on your server is lost, your business is going to feel it. The hard drive might contain years of client data, the database for your management software, or marketing materials created over a year by your marketing team. Data loss can change your business suddenly and in drastic ways.

Depending on the type and severity of the event where you lose your data, you could fall out of compliance with the regulations your business operates under, causing additional headaches. Data loss isn't exclusive to internal IT problems, if one of your staff has a mobile device or laptop stolen, it could expose sensitive data.

Just Prevent Data Loss

The theory becomes simple then, just don't lose data. Do what you can to protect it.

Fortunately, there are plenty of solutions created to stem the problem of data loss. One of those solutions is to securely back up your data.

Industry best practices dictate that your data should be stored in three places. We call this the 3-2-1 rule. It is defined...

Read the Rest Online!
https://dti.io/backuphelps

Cybersecurity Tips

Protecting Devices and Data Outside of the Office

The transportation of equipment is becoming very common, making the protection of these devices and data during their travels extremely important. Learn some of the best practices for safely and securely transporting devices and data.

https://dti.io/protectoffice

Get our Cybersecurity Tips to your inbox weekly!

Each week we send an email with **FREE** cybersecurity tips to help you to avoid a data breach. These tips can be used to educate yourself and your employees on security best practices.

Sign up today!
https://dti.io/gettips

Marketing Ideas & Tips for Your SMB

Direct Mail Isn't Dead... Here's How to Use It Effectively

Print marketing is alive and well and sending direct mail pieces through the mail can be an effective way to target leads, prospects, and clients.

There's something special and unique about getting something in the mail that resonates with people, even if it's "just" marketing materials. This greater investment into communication adds a personal touch to your marketing and gives recipients a tangible reminder of your business that won't get lost in their email or buried in their social media feed.
Here's how you should be using direct mail as a part of your own marketing strategy.

Effective Direct Mail Marketing Mediums

As you probably know, you have a lot of flexibility when it comes to direct mail marketing. However, the costs can definitely add up!

Here are five great, relatively affordable options that a small to medium-sized MSP can take advantage of:

- **Letter -** Letters are a great way to introduce your business to a potential prospect in your area. You can also use them when you want to include a lot of information about a product or service you offer. When using them, make sure they are branded with your logo and are signed as coming from a prominent member of your team, like your CEO or a head salesperson.
- **Postcard** - Postcards command attention with their oversized image, drawing in the recipient to read the marketing message.
- **Newsletter** - Printed newsletters draw attention like postcards do and have the added benefit of tending to stick around the office to be read at leisure. As a result, your target is effectively hanging on to your marketing and generating more impressions for you!
- **Deliverable** - Send a deliverable to your promising prospects with an accompanying letter. Consider including a brochure or a case study!
- **1% Kit** - A package full of branded goodies and in-demand office supplies is sure to leave an impression! While it's a bit more costly to send one of these compared to our other suggestions, things like mouse pads, calendars, and mugs have a chance to be used quite frequently; when they're branded, the user gets a reminder of your company every time they use the item.

Provide a Direct Line to Your Website

Your marketing should always direct back to your website; just because your marketing materials aren't on a digital medium doesn't mean you shouldn't be trying to get recipients there. Here are two effective ways to do so:

- **QR Codes** - Many mobile phones have QR code readers built into their...

Read the Rest Online!
https://dti.io/directmail

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

Visit us **online** at:
newsletter.directive.com

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