TECHMinutes
January 2021
Your Small Business Technology Information Source!

This Issue:

What Exactly is Software-as-a-Service?

Businesses have many problems they need to solve. With technology, the process typically starts with identifying a problem, researching solutions, and finding one that will successfully work to solve the problem. Traditionally, when dealing with technology, a company would procure the hardware and hire technicians to implement the solution and deploy the services needed. If they had to borrow money to do it, they would because the profits would presumably be more than the payments even with banks tacking...

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

Should auld acquaintance be forgot, we hope you don't forget our managed services! Have a happy and prosperous New Year!

Let's Take a Look at Some Popular Internet Scams

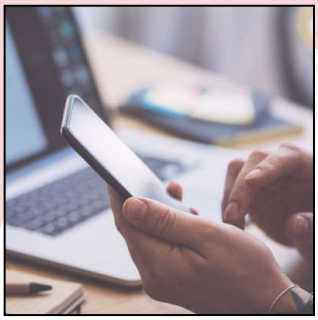
The year 2020 hasn't been kind to many people. Between the COVID-19 pandemic, the resulting economic downturn, and the people looking to take advantage of these negative circumstances, it's hard to know what to do to keep from becoming a victim. What helps is to take a thorough examination of where your business' weak points are. This month, we thought we would take a look at cybersecurity by examining the perpetrators and their methods.

Phishing

We can't even talk about digital threats without first talking about phishing. Phishing has always been a good method for hackers to gain control over accounts, but since a lot of the security software that is defending current computer systems is extraordinarily good when compared to security software of old, it typically takes a user to trigger a network security breach. Phishing is the most used method, accounting for over one-third of all security incidents.

(Continued on page 2)

Mobile Devices in the Workplace



Smartphones are everywhere. You go to the supermarket, people are on their phones, you go to the gym, people are on their phones. Go into the office? People are constantly on their phones. All that phone use cannot be in the best interest to organizational profitability. The question becomes, do smartphones help or hurt business? Let's get into it.

Smartphones at Work

Let's start with the trickiest bit of this first. Smartphones are a distraction, pure and simple. In fact, according to one survey, employees average about 56 minutes per day on their phones while they are in the office. This equates to a massive productivity leak for many businesses, but just when you think it isn't equitably fair for the employer to pay for time employees spend scrolling through Twitter, Facebook, and Instagram, responding to personal emails, and browsing websites blocked by the company's content filter, employers aren't totally innocent in this situation.

The modern employer is the first person to take advantage of the computing prowess of these devices. Since the modern company tries to do more with less, many employers expect their workforce to always be available; and, that means always. Moreover, managers and executives aren't any different: they are always on their smartphones too!

(Continued on page 3)

25+ YEARS IN BUSINESS
est. 1993

Ease Your Mind with Managed IT Services

Your business relies on technology to keep operations moving, but your technology relies on you to stay functional. While many small businesses will choose to forsake an in-house IT department in favor of a self-service model, this is a costly maintenance practice that could put your IT in jeopardy. Instead, your organization should invest in our managed IT services, which have the possibility to show your business an entirely new way of managing technology assets.

Instead of taking a break/fix approach to IT, managed technology services take preventative measures to keep problems from escalating into major disasters. Here are three ways that managed IT services can help your business.

Reduce Your Costs

One of the biggest ways you can save on your IT is by implementing managed services. Due to the way managed services work, you get a service for a monthly fee. Now, compare this to the usual way of managing technology. When your technology breaks, instead of reaching out to a company that can diagnose and fix your problems for a steep cost, a managed service provider can administer the care needed as per your service level agreement.

Furthermore, the majority of problems can be prevented through careful maintenance and management, which is something that a break/fix IT provider won't tell you. After all, they profit from your technology constantly breaking down. Managed IT providers want to save your business money through preventative maintenance. This means minimal hardware replacements, as you'll only need to replace technology that's in danger of an imminent failure.

Waste Less Time

Chances are that your business doesn't have an internal IT department, and even if you do, it's probably buried in work that nobody has time to get to. When there's too much work that needs to get done, it's easy to accidentally cut corners in order to...

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

Let's Take a Look at Some Popular Internet Scams

(Continued from page 1)

Phishing works with the assumption that the user is the weakest link and can be manipulated and coerced into providing the means to gain access to a computing environment. With so many successful breaches resulting from phishing attempts, you'd have to agree that this strategy works. There are many different types of phishing messages, but the main strategy is to flood people's email and messaging systems with messages that seem to come from a reliable source, but actually carry malware and other undesirable attachments. Some target individuals, but the lion's share are more like a phishing net than a phishing lure.

Once the hackers hook their victims, they can then access secure computing resources or deploy their malware payload. Phishing attacks typically use current events to present scammers more opportunities for "success". More often than not these attempts are fruitless, but when someone slips up and clicks on a link or downloads an attachment, they are in business.

Loan and Payment Card Scams

Another prevalent scam is the loan or credit card scam. This is one where a seemingly trusted organization floats a line of credit to someone that typically wouldn't qualify for it. This is enticing enough for the recipient to go through the motions trying to get the money. Oftentimes, part of the ruse is that the recipient of the loan or payment card has to pay some money as a down payment in order to receive the promised sum of money. The user will pay and that will be the end of it, hopefully.

Some people that get roped into this scam provide scammers with access to their financial accounts and find that there are mysterious withdrawals from their accounts. These scams are more likely to work in recessionary periods as many, many people are looking for a way to make ends meet. You may think that these types of schemes are clear as day and wouldn't work, but you would be surprised what people will do when they are under financial duress.

Fake Antivirus

This scam is a tried and true one. You will get a popup while you are surfing the web that looks urgent. It says something along the lines of "You've been infected! Download our product to remove the dangerous virus before it is too late!" This message flashing on your desktop is enough to get people to panic and make a grave mistake.

Users that would fall for this scheme could get lucky if it is only a hoax, or they could be in a world of hurt when their files or drives are encrypted and held for ransom. That's why it is imperative to keep your head when confronted with abnormalities online. Impulsive action almost always results in worse results than deliberate action. The best way to avoid the risks carried out by these pop ups is to not click on them and to add an extra layer of protection to your antivirus that will help ward against malware deploying pop ups.

Fake News Scam

Another noteworthy scam that is all the rage among hackers in 2020 (and going into 2021) is the fake news scam...

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

Mobile Devices in the Workplace

(Continued from page 1)

Some organizations feel the need to try and strategically design policies to keep people from using their personal devices for personal use on company time. These same people don't have a problem with them using these devices for the benefit of the organization, just not for personal gain. This is where policies go wrong. They create archaic and completely unrealistic policies and are shocked when even their best performers can't avoid their phones for long.

If you want your staff to limit their phone use at work, you have to make that clear. Some companies have implemented a policy that provides small breaks in which they can use their phones, but most companies have come to understand that this isn't a trend and that phone use is part of day-to-day life. Locking down people's ability to connect with the outside world for eight (or more) hours a day is only going to serve to bring negative reviews from your team, so your best bet is to embrace it, and realize that as long as your expectations have been communicated properly, most employees won't take advantage.

Smartphone Use Outside of Work

While the smartphone may be a bit of a distraction to your in-house staff, what happens the moment people leave the confines of your business? They use their phone. In fact, I doubt very much if they make it out to their car or onto the train without a full assessment of the messages sent by applications, people, and others. How long do you last without checking yours?

This brings us to the point that needs to be hammered home. The more people use mobile devices, and specifically smartphones, the more they are willing to use it for work, off the clock. You don't think this is true? If you are a...

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

Why You Need to Prioritize Backup and Recovery

It doesn't take a lot of consideration to know that your business is extremely limited without its data. There are dozens of antivirus solutions on the market for this very reason. One of the best ways to protect your digital assets is to back up data using a reliable backup platform. In today's blog, we'll go over a few basic considerations to make if you want a data backup that you can trust.

Secure Your Data with Multiple Backups

Your backup is more than just an insurance policy for your business operations. In the case of a disaster or other cause of data loss, your backup essentially takes your business' place, allowing you to recover more quickly with fewer consequences. This means that your backup needs to be kept safe. The first step to doing so is to make sure your data backup is stored separately from your primary data storage. We suggest using the 3-2-1 rule, which is three total copies of your data, with two available onsite and one stored offsite. This will help you avoid a situation where the same disaster that damaged the original data wipes out your backup too. Cloud-based backups are especially effective at preserving your data in a major disaster.

Create a Disaster Recovery Strategy

How quickly could your business return to full operation after undergoing a disaster? While establishing an off-site backup to preserve your data is a good start, you also need to have a plan in place that will allow you to put that data to use as quickly as possible. This is where it is useful to have a disaster recovery strategy, as it allows you to proactively prepare for circumstances that would otherwise lead to data loss and wasted time and productivity.

Make Sure Your Backup is Working

Imagine what it would be like to go through the entire process of establishing an offsite backup, only to have it fail when you're relying on it. Fortunately, this can be avoided through some simple tests to ensure that the backup works effectively. You'll be happy you did if you ever find yourself in the position that you need to restore from a backup and it works.

Share this Article!
https://dti.io/prioritizebdr

Cybersecurity Tips

Cybersecurity Resolutions

A new year generally brings some important resolutions and goals to help better ourselves. With the many cybersecurity threats bearing down, now is the time to add some cybersecurity resolutions to your list.

https://dti.io/cyber20

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

Top Fourteen SEO Frequently Asked Questions

Looking to rank your website higher, but not sure where to start? Here are fourteen frequently asked questions that should better help you understand what SEO is and how it can help your business attract traffic to your website, increase your rank, and ultimately generate leads.

Top Fourteen SEO Frequently Asked Questions

1. Question: Why is SEO important?
Answer: SEO is important because it is the primary method to drive organic traffic to your website. The more traffic you have to your site, the more opportunities to engage and convert visitors into customers. Moreover, the more traffic you have to your site that stays, signals to Google that your site is relevant to the questions searchers are looking for.

2. Question: Why is Organic Traffic important?
Answer: Organic traffic is important because it is focused and the result of a user's specific search intent. This makes it more likely they will click on your link in search of the information they are looking for and convert if they go to your website.

Extra Question: What does SEO stand for?
Answer: Okay, this question isn't super common, but we wanted to make sure we answered it here. SEO is an acronym for Search Engine Optimization. Related terms include PPC (Pay Per Click) and SEM (Search Engine Marketing).

3. Question: What is SEO?
Answer: SEO is a digital marketing tactic designed to optimize a website's search result position. The goal of SEO is to raise your page position (rank) so that you are above and seen before your competitor's listings by making it more visible on a search result page.

4. Question: How does SEO work?
Answer: Basically, the goal of SEO is to help Google better understand your website and therefore what services you're offering. This is achieved in a variety of methods but two main metrics are authority and relevance. The more authority (testimonials, reviews, backlinks) and relevancy (content) you have, the higher your website positioning will be.

5. Question: What is page position?
Answer: Page position is the location your website is at as the result of a search. For example, a featured snippet is position 0, because it is located at the top of the search results page before the first search result (position 1) begins. On average, position 11 will put you on page 2 of a Google search result.

6. Question: What is a search result page?
Answer: A search result page (SERP) is the page generated by a search engine (usually Google) in response to a query (question) by a user.

7. Question: What is Technical SEO?
Answer: Technical SEO is also known as On-page SEO. A feature of technical SEO is that it is more focused on how search engines 'read' the page than human users. However, if you follow best...

Read the Rest Online!
https://dti.io/14seofaqs

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