



T. Daniels Consulting

THE T. DANIELS TIMES



Microsoft Partner

Silver Cloud Platform
Silver Small and Midmarket Cloud Solutions

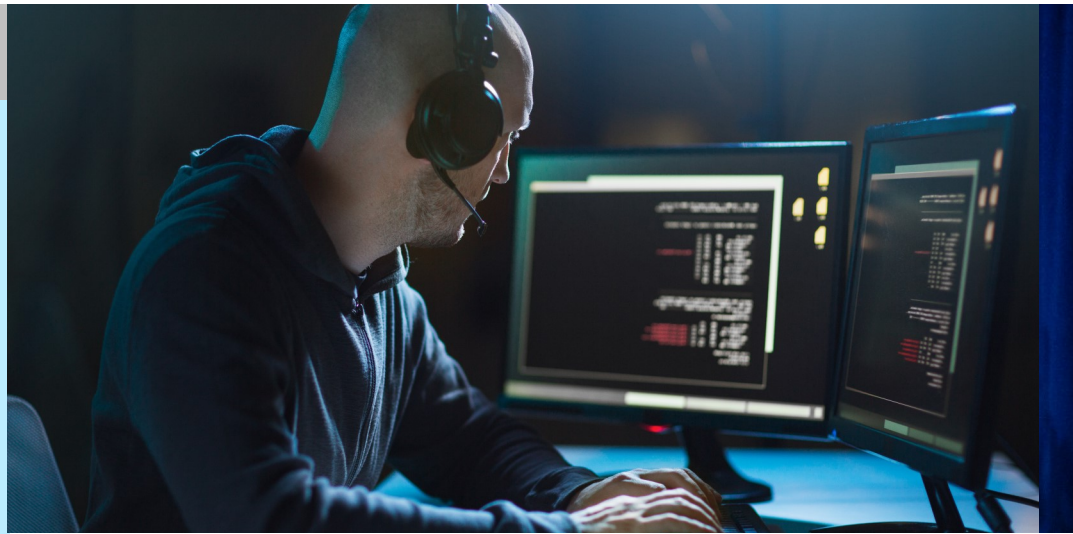
What's New

There have been many things learned during the COVID pandemic. One we can all likely agree on is that technology is a critical component of our businesses and there are many tools available to help us remain 'open' even when the physical office is closed.

One of these tools is a VoIP phone system which allows you and your team to make and receive phone calls from outside of the business walls.

What makes T. Daniels Consulting's VoIP service different than all the rest? As a VoIP system is an integral part of your overall network, you need someone who knows and understands network management to receive the quality and full benefits of your system. That is what makes us unique. We don't just sell the phone system; we are experts in network management.

To learn more, contact us at 810-629-0131 or e-mail us at info@tdaniels.com.



3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security *once*. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years. Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up-to-date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand The Threats

It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cybercriminals rely on social engineering.

The most common form of social engineering is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file. Cybercriminals have gotten VERY

July 2020



This monthly publication provided courtesy of Timothy D. Ricketts, President of T. Daniels Consulting.

"Thank you for the confidence you have given our entire team to manage and protect your valuable assets. We take great pride with our goal to exceed your expectations every day!"

Continued on pg.2

Continued from pg.1

sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And Update

From software to hardware, you must stay updated. There is no such thing as “one-and-done” when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that

you need to replace that piece of hardware. The same applies to software.

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring

When it comes to the security of your network and overall business, being proactive can make a huge difference. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, “How am I going to do all this?” You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

“Proactive monitoring means your network is being watched 24/7.”

Free Executive Guide Download:

The Business Owner's Guide To IT Support Services And Fees



You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other “gotcha” clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at:

<https://www.tdaniels.com/itbuyguide720/>

Shiny New Gadget Of The Month:



FitTrack – A Smart Scale That Does More

The bathroom scale isn't always the most useful device in the home. FitTrack is a smart scale that aims to change that. It's a different kind of bathroom scale that gives you *much* more than a single number.

Traditional bathroom scales don't tell you anything about what's happening in your body. FitTrack *does*. It gives you an "inside look" into what's going on inside your body. It measures your weight, body fat percentage, body mass index, muscle and bone mass, hydration and more. In fact, it tracks 17 key health insights.

The advanced scale pairs with the FitTrack app, which you can download to your smart phone and connect to the smart scale. All you do is step on the scale with your bare feet – the scale actually reads electrical signals from your body – and it sends the results to your phone. Simple and useful. Learn more about FitTrack at bit.ly/2VOg7Vs.

3 Signs It's Time To Upgrade Your Telecommunications

Telecommunication technologies have rapidly advanced in recent years with the maturity of Voice over Internet Protocol (VoIP), the strategy of software virtualization, and the birth of Unified Communications (UC). How do you know if it is time for your company to make a change? Read the **3 signs** that it's time to upgrade your telecommunications.

1. VOIP can save 50% or more over your current phone plan.

You are wasting money on what it takes to keep your current system up and running.

As your old systems age, go end of life, and become obsolete with the advancement of new technologies, you are faced with the challenge of maintaining functionality and more importantly, security and associated cost.



Older telecommunications products were built with proprietary hardware and software that can be cost prohibitive to maintain. Often, vendors that provided you with these systems can only offer expensive overhaul solutions.

2. You Have Outgrown Your Current System.

Your business has grown since the time when you bought your current system.

Maybe you have expanded to new locations, hired more employees, or have additional feature requirements. Any and all of these circumstances were not considered in the deployment of your current system. **Are you trying to stretch the old technology to do things that it was never meant to be capable of doing?** Much like a



pair of pants that shrank in the wash, your current system just doesn't fit like it used to.

3. You Are Wasting Your Team's Talent On Upkeep.

Your team spends more and more time maintaining legacy

communication systems and making sure that everything is working. If this seems like a waste of talent, that's because it is! With today's newer communications platforms, you are able to manage the day to day operations with ease and keep your employees efficient and productive.



Another important consideration is integrating the phone into your network. Take for example the last time you purchased a new printer or copier and recall how it didn't 'just work' by simply plugging into the wall. Most likely you called a network specialist to help the printer guy. That's because printers (*and phones*) need to be securely installed into your network. Most phone/printer vendors don't know how to do it correctly. This is the reason you want a telephony engineer from T. Daniels to properly configured and secured the device, otherwise, they are an open invitation for cybercriminals to access your network.

You need a VoIP provider that not only knows phones but also is network certified. That's the T. Daniels difference. When you partner with us, you get a team of experts with the network knowledge to ensure the security, stability, and efficiency of your VoIP system. To learn more and get a free VoIP assessment, visit:

<https://www.tdaniels.com/voip> or call us at 810-629-0131.

The T. Daniels Difference



For over 25 years, T. Daniels Consulting has provided Small and Medium sized organizations with excellent customer service. Our Microsoft Certified Professionals and Engineers have an average 10 years' experience benefiting you by fixing problems quickly and correctly the first time. No other competitor comes close to our level of knowledge, experience and professionalism. We are continuously adding new and improved services to meet your ongoing needs. We never stop improving. That is the **T. Daniels Difference**. Thanks to all of our customers for making us one of Michigan's fastest growing IT consulting and service companies.

■ 3 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest.

Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then

you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly and working as intended.

But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. *Inc., July 30, 2019*

■ How Malware Can Cripple Your Business

Every year, the number of malware attacks on small businesses increases.

Symantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. *Small Business Trends, Oct. 12, 2019*

