T. Daniels Consulting

THE T. DANIELS TIMES

Microsoft SMB Cloud Champions Club

Microsoft Partner | Silver Cloud Platform, Silver Small and Midmarket Cloud Solutions

What's New

Cybercriminals are very good at getting personal information from unsuspecting victims, and the methods are getting more sophisticated as technology evolves. Further complicating this is that criminal groups are increasingly switching to COVID-19 themed lures for phishing and exploiting employees' concerns over the pandemic and the safety of their loved ones.

T. Daniels Consulting's unique multi-factor authentication solution (MFA), **SecureFactor,** reduces network disruptions and data breaches arising from weak or stolen credentials.

Learn more on **Page 3, call 810-629-0131 or e-mail us at info@tdaniels.com**

August 2020

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

"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!"

The #1 Mistake Companies Make With Their IT

If you're like many businesses today, there's a good chance you've made this one mistake with your IT security: you don't budget for it.

Or if you do budget for it, it's not enough to *really* protect your business.

Time and time again, business owners decide NOT to invest in IT services. Instead, they go it alone or skip it completely.

Or they might approach an IT services company and ask, "What do you charge for your services?" They don't ask, "What will I get for my money?" or "How can you meet the needs of my company?"

This is a backward approach to IT – and it's a big mistake.

The fact is that a lot of business owners don't take IT seriously. They think that because they haven't been hit by a data breach or a malware attack that it will never happen to them. That's another big mistake. Just because a business hasn't fallen victim to a cyber-attack DOES NOT mean they're safe.

It's the opposite.

When you hire an IT services company, what *do* you get for your money?

The honest answer is that it depends on your specific needs. Many IT services companies offer everything from basic to advanced network security. You can expect services like:

- Cloud backup
- Data protection
- Data monitoring
- Threat detection
- Technology maintenance
- And more!

Continued on pg.2

Continued from pg.1

Everything is designed to protect you, your network, your technology, your employees and your business as a whole. It's all about giving you the information and resources you need so you can worry less about outside threats and focus on your customers and the success of your business.

When you're invested in good IT security, you shouldn't even know it's there. It runs in the background like a quiet but powerful electric motor. It's there when you need it, and it's there when you're not even thinking about it.

For some business owners, this is a tough pill to swallow. They don't have something tangible in front of them that they can see 24/7. A lot of business owners like to be more hands-on. They like to see what their money is buying.

The great thing is that a good IT services company will provide you with something tangible. If you want to see what is going on behind the scenes of your IT security, they will give you a complete report. Every day (or week or month), you can have an e-mail delivered to your in-box that breaks down exactly what your IT services firm is doing for you.

You can see things like the threats they blocked from getting through. You can see when they performed system maintenance or when your data was backed up. You can customize these reports to your needs. Basically, you can see what you're paying for and how it's working. This is the very definition of "peace of mind."

Today, none of us can afford to skip out on good IT security. We can't wait to react until something happens. Because when something does happen, it's often too late. The cybercriminals have done their damage and moved on. Meanwhile, your business comes to a screeching halt, and you have to pay the big bucks to get everything back on track – if you *can* get back on track.

Some businesses don't get back on track. They are forced to close after a cyber-attack because they don't have the money or resources to recover. The damage is simply too much and the cost too high. If they had invested in IT security upfront, it might be a different story.

Don't get caught off guard by a data breach, malware infection, hacker attack or data loss due to technology failure or natural causes like flood or fire. It's time to take your IT to the next level. Protect your business the right way and avoid the mistake so many others make when they avoid the investment in good IT.

Work with an IT services firm that takes your business as seriously as you do.

"We can't wait to react until something happens. Because when something does happen, it's often too late."

Free Executive Guide "What Every Small-Business, Local Government and Non-Profit Must Know About Protecting And Preserving Their Organization's Critical Data and Computer Systems".

This executive guide will outline in plain, nontechnical English the common mistakes that many small-medium organizations make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

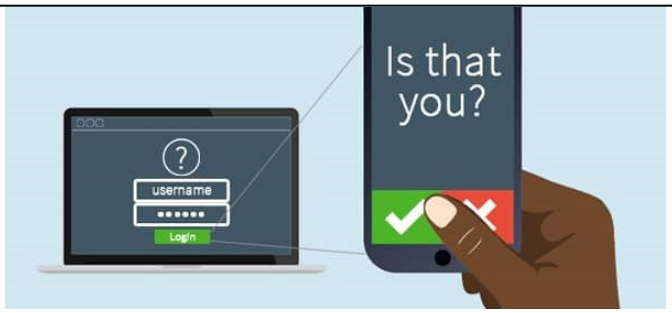
Download your FREE copy today at https://www.tdaniels.com/protectdata820/ or call our office at (810) 629-0131

Shiny New Gadget Of The Month:

The Manta5 Hydrofoiler

If you could ride your bike on the water, would you? Thanks to the Manta5 Hydrofoiler XE-1, *you can*. The Manta5 Hydrofoiler XE-1 is a high-performance watercraft for people of all ages. The minds behind Manta5 wanted to bring cycling to the water – and they succeeded.

The hydrofoil design helps keep you balanced while you pedal across the water, similar to how you pedal on a bike. You can use it on the ocean, in rivers and in lakes. Learning to ride takes practice, but once you get the hang of it, it's a breeze! It won't be long until you're jetting across the water – on your own power! There's even a small electric motor that brings you up to speed if you need it. Take your summer to the next level and learn more at https://manta5.com/



Lock Down Your Login With Multi-Factor Authentication (MFA)

You may have already noticed that a lot of your accounts are now requiring multiple methods of verifying your identity when you login. No longer do you just enter your username and password to get into your email, bank account, or online medical records. You now also need to input a short code that is texted to you, generated by an app, or emailed. This is called multi-factor authentication (MFA).

What is multi-factor authentication? MFA consist of three basic things that when combined verify someone's identity. The three things are: something you know, something you have, and something you are.

This may seem like a giant hassle, especially when you're setting up these multiple verification methods, or if you need to run to find your cell phone for that text message code. But it's making your accounts even securer by requiring multiple pieces of information or identification from you. This lessens the likelihood that someone will have all the pieces of data they need to hack an account.

A hacker may have your username and a list of your commonly used passwords, but if they don't have the third or fourth verification steps, they'll be stopped in their tracks. And this is a very good reason to not be afraid of using MFA!

Why is MFA such a big deal?
MFA can stop many common brute force attacks and phishing attempts. All it takes is a hacker to compromise a single email account in your organization. Suddenly coworkers start receiving legitimate-looking emails from a person they trust asking for sensitive information. Then the entire organization can be compromised.

The reality is that many traditional cybersecurity measures can be compromised without MFA. Anti-virus software, firewalls, encryption tools, network monitoring solutions, and more can all be bypassed if hackers compromise them and gain credentials to privileged user accounts. MFA is a beautifully simple solution to lock down accounts even further. And it's often not that hard to implement either.

4 reasons why multi-factor authentication is so important for your business.

1. **Identity theft is easy, and it's a growing threat** to all businesses. MFA makes identity theft harder.
2. **Small businesses are being targeted at a growing rate by cyber attackers.** New security measures are not for enterprise-class organizations only. MFA is simple and relatively easy for small organizations to roll out.
3. Other cybersecurity tools and solutions, like anti-virus and firewalls, **are only as strong as their user authentication procedures**. MFA can make your existing perimeter security stronger.
4. **MFA is already becoming ubiquitous.** People are accustomed to authentication procedures in their personal as well as professional lives. Social media, banking, gaming, and email platforms have all rapidly adopted MFA. Bringing it into your workplace is a no-brainer.

To learn more, visit: https://www.tdaniels.com/secure-factor/ or call us at 810-629-0131.

The T. Daniels Difference

25 YEARS
1994 ~ 2019
T. DANIELS CONSULTING

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.

The 'Not Me!' Problem …

Remembering 24 different passwords, memorizing four PIN numbers and installing updates all the time is frustrating enough. Many of us also have to remember the code for the door, the alarm code for the alarm panel next to the door, the secret password to tell the alarm company, the passcode to your phone, the garage code … You get the idea.

This logic is based on a time when threats were more "real," like the idea of someone robbing our house. In 2020, these types of threats are statistically less likely to happen than virtual threats like fraudulent credit card charges, data loss and identity theft. In fact, cyberattacks occur three times as often as home burglaries in the United States, according to a 2016 study by the University of Kentucky.

It's important to avoid the "Not me!" approach to this shift. Businesses say this all the time: "I'm too small for anyone to want to steal my data. I have a good firewall, hourly backups and a great IT support partner – no one will steal my files."

But the truth is that businesses with under 100 employees are low-hanging fruit for cybercriminals – yes, that's a lot of you! It can happen to you, so you must approach all aspects of physical and electronic security with the attention they deserve in today's business world.

Do You Have The Right Business Insurance To Protect Your Company?

There are several types of business insurance on the market. Each one serves a different purpose, and getting the right insurance can save you the major headache that comes with not having insurance or having the wrong type of coverage. While we can't list them all here (there are too many!), here are a few examples:

Commercial property insurance – This is one of the most important forms of insurance. It protects equipment in the business against damage or loss.

General liability insurance – This is another important one. It helps cover injury and legal expenses should someone get hurt on your business's premises.

Cyber-insurance – This offers protection should you fall victim to malware, cyberattacks and other digital threats. Basically, if your business is connected to the Internet, you need extra protection.

Umbrella insurance – This is another layer of protection on top of existing insurance. Exact details vary by plan, but it can often protect you if you need to pay legal fees or costs related to building or equipment damage. *Small Business Trends, May 13, 2020*