T. Daniels Consulting

THE T. DANIELS TIMES

Microsoft SMB Cloud Champions Club

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

Did You Know?

Our Blog is filled with helpful technology tips and insights for your business.

We post new articles that provide valuable information for your business almost every day. You can sign-up to be notified of new topics when they are posted or you can visit https://www.tdaniels.com/blog.

Here are a few examples of the kind of information that is available:

- **Recent Massive Data Breach Attacks T-Mobile Company:** *https://www.tdaniels.com/t-mobile/*
- **Microsoft Teams Adds A Number Of New Features:** *https://www.tdaniels.com/teams-features/*
- **Has Your Bandwidth Slowed Down? It Could Be Proxyware:** *https://www.tdaniels.com/proxyware/*

October 2021

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

"As a business owner or leader, you don't have time to waste on IT issues. That's our expertise. Call us and we will put an end to your IT problems so you can stay focused on what's important–growing your business."

Protecting Your Business From Data Disasters

Data is everything to a company in this day and age – which means if you lose access or control of your data, you lose everything.

As dramatic as that might sound, the data backs that up. According to several sources, 93% of companies, no matter how big they are, are *out of business within one year* if they suffer a major data disaster without having first formulated a strategy for combating it. And since 68% of businesses don't have any sort of plan for that worst-case scenario, that means losing data would be a death knell for most of the businesses in the country.

Fortunately, your business does not have to be one of them. By taking the following steps, you can ensure that you have a rock-solid disaster recovery plan in place.

Step 1: Know How A Disaster Recovery Plan Is Different From A Business Continuity Plan

The main difference between these two types of plans is that while business continuity plans are proactive, disaster recovery plans are reactive.

More specifically, a business continuity plan is a strategy by which a company ensures that, no matter what disaster befalls it, it can continue to operate and provide products and services to its customers. A disaster recovery plan, on the flip side, is a strategy by which businesses can back up and recover critical data should it get lost or held for ransom.

So, now that we have a clear, concise understanding of what constitutes a disaster recovery plan, we can dive into the steps necessary to create one.

Step 2: Gather Information And Support

In order to get the ball rolling on your disaster recovery plan, start with executive buy-in. This means that everyone, from the CEO to the entry-level employees, needs to be brought

Continued on pg.2

Continued from pg.1

in on executing the plan in case your company suffers a data disaster. When everyone is aware of the possibility of a data disaster, it allows for cross-functional collaboration in the creation process – a necessary step if you want to prevent breaches in all parts of your systems.

You need to account for all elements in your tech systems when you're putting together your disaster recovery plan, including your systems, applications and data. Be sure to account for any issues involving the physical security of your servers as well as physical access to your systems. You'll need a plan in case those are compromised.

In the end, you'll need to figure out which processes are absolutely necessary to keep up and running during a worst-case scenario when your capability is limited.

Step 3: Actually Create Your Strategy

When everyone is on board with the disaster recovery plan and they understand their systems' vulnerabilities, as well as which systems need to stay up and running even in a worst-case scenario, it's time to actually put together the game plan. In order to do that, you'll need to have a good grip on your budget, resources, tools and partners.

You might also want to consider your budget and the timeline for the recovery process. These are good starting points for putting together your plan, and doing so will also give you an idea of what you can tell your customers to expect while you get your business back up to full operating capacity.

"93% of companies, no matter how big they are, are out of business within one year if they suffer a major data disaster without having first formulated a strategy for combating it."

Step 4: Test The Plan

Even if you complete the first two steps, you'll never know that you're prepared until you actually test out your disaster recovery plan. Running through all the steps with your employees helps them familiarize themselves with the steps they'll need to take in the event of a real emergency, and it will help you detect any areas of your plan that need improvement. By the time an actual data disaster befalls your business, your systems and employees will easily know how to spring into action.

So, to review, these are the quick actions that you and your employees will need to take in order to make a successful, robust disaster recovery plan:

- Get executive buy-in for the plan.
- Research and analyze the different systems in your business to understand how they could be impacted.
- Prioritize systems that are absolutely necessary to the functioning of your business—i.e. your accounting system.
- Test your disaster recovery plan to evaluate its effectiveness.

Complete these steps, and you can ensure that your business will survive any data disaster that comes your way.

As A Business Owner or Manager, Do You Ever Wonder If Your Network Is **Secure From Hackers, Scammers and Thieves?**

As 80% of all data breaches involve lost or stolen passwords which means it's likely your network is NOT secure.

A recent survey showed that 84% of business owners know weak passwords can lead to a cyber-attack; yet, 46% of these same owners believe they can't force their employees to have strong passwords.

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your business, obtain your passwords, and steal your data. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself on how to PROTECT what's yours!

Read more and learn how to prevent from becoming a statistic at: https://www.tdaniels.com/mfa-survey/

Shiny New Gadget Of The Month:

The LINK AKC Smart Collar

The world can be a dangerous place for a pooch who doesn't know any better; so, it's best to know how to keep tabs on your canine companion in case they bolt. That's where the LINK AKC smart collar comes in.

This smart collar is a comfortable and safe tracking alternative for your pooch. The LINK AKC smart collar comes equipped with several other useful features, including but not limited to:

- Activity monitoring and sound training specific to your dog's breed
- Temperature alerts if your dog is too hot or cold
- A place to digitally store vet records
- Waterproof features for up to 30 minutes in three feet of water

If you want your dog to be the goodest, highest-tech boy or girl out there, this collar is for you!

This One Thing Prevents 99% of Hack Attempts on Businesses

Cybercrime is on the rise.

Economies and businesses around the world face new and upcoming challenges all the time but probably none have been as disruptive as cybercrime has been in these past few years. It is by far the biggest threat to US businesses today.

Whether you run a small business or large, with thousands of successful hacks taking place every day, you are a potential target and under common threat of cyberattacks. Cybercriminals and hackers are updating their tactics and approaches and becoming better and better by the day.

While there is no fool-proof way to protect yourself and your company completely, one security method has shown to work effectively against hackers' breach attempts.

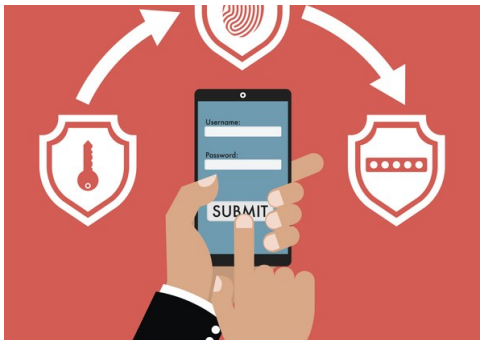
According to tech giant Microsoft, multi-factor authentication (**MFA**) is able to **block 99 percent** of hack attempts[1]. Microsoft experiences over 300 million fraudulent sign-in attempts to their cloud services every day and MFA proves to be the best way to obstruct 99 percent of these attempts.

A common example of MFA, which you may have experienced, is when you log into your banking account. Chances are it will always ask you to confirm your identity via an extra security measure such as providing a one-time password (OTP), or code, sent to your mobile device.

This is what MFA is, it is a verification process that requires a separate channel to authenticate your identity when logging into your accounts. An effective technique that can be applied to all your other accounts as well, such as social media accounts, emails, and software applications.

Why Multi-Factor Authentication (MFA) Works

When hackers or cybercriminals try to breach



your account, they typically rely on the credentials of their targeted account. They may manage to get their hands on them through various hacking techniques.

Hackers typically cannot and do not go through the efforts of fighting MFA because it is incredibly difficult and close to impossible. Which makes it an unviable pursuit for them, and they usually give up on their hack attempt.

Multi-factor authentication may seem like an inconvenience, but it is a minor inconvenience compared to the major hassle of a breach.

So, now that you know why MFA is so important and so easy to implement, the question you need to answer is no longer why should you enable MFA, but why wouldn't you enable MFA?

If you do not have a good answer that has been vetted by a security expert, then you need to get MFA setup on your systems today and keep your data safe. Read more about the importance of MFA here or if you are ready to enable MFA for your business, visit: https://www.tdaniels.com/secure-factor/ or contact us at (810) 629-0131 and we will be glad to help.

[1] *Source: https://bit.ly/2YDcHsJ*

The T. Daniels Difference

25 YEARS
1994 ~ 2019
T. Daniels Consulting

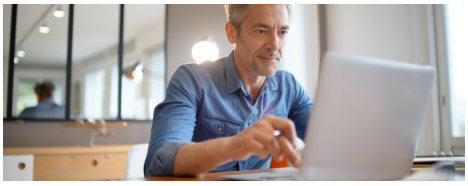
For over 27 years, T. Daniels Consulting has provided Small and Medium sized organizations with excellent customer service. Our Microsoft Certified Professionals and Engineers have an average 15 years' experience benefiting you by fixing problems quickly and correctly the first time. No other competitor 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 Digital Disruptions That Affect WFH Employees And How To Avoid Them

As more employees work from home, the risk of cyber-attacks grows. In 2020, between the months of March and July, nearly half of all businesses dealt with some sort of digital disruption. Some of the most common digital disruptions were:

Worker Productivity Losses

When hackers infiltrate company computers, they might steal employee identities. This won't hurt your business directly, but it will indirectly, as workers have less time for work while they grapple with their identity being stolen.



Internet Of Things Infiltrations

Now that so many "smart" devices can be hooked up to a central server, there are more avenues than ever for hackers to gain access to sensitive company data.

Ransomware Attacks

Businesses of all sizes are falling victim to ransomware attacks, but it's the small and mid-size ones on a tight budget that really suffer from the fallout.

To stop these kinds of attacks, educate your workforce on best practices for avoiding hackers and make sure their systems are up-to-date with good cyber security software. Nothing is bulletproof, but you can do a lot to protect your company.

"It's guaranteed for the life of the product which, obviously, ended when it broke."

CartoonStock.com

5 Tips For Millennial Entrepreneurs From A Millennial Entrepreneur

Millennial entrepreneurs are more diverse than entrepreneurs of any other generation, with a greater portion of them being women and people of color than ever before. But what does it take for a millennial to succeed in this brave new world of business?

1. Remember that although older business owners may have valuable insights, they might not understand how entrepreneurship works in the digital age.
2. Know how to do every job in your business; after all, you'll have to do them all when you start out!
3. Find a mentor, someone who is where you want to be one day, and learn from their successes and failures.
4. Don't take advice from people who haven't been where you are – even if the advice is well intentioned and from people you care about.
5. Do not let people judge you for your age. Being in the know about the latest tech – because of your age – is a tremendous advantage in today's marketplace.