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:

- **Another Malware Evolves To Gain Access To More Systems:** *https://www.tdaniels.com/purple-fox/*
- **FREE E-book- Cloud Migration Essentials:** *https://www.tdaniels.com/cloud-migration-essentials/*
- **Identity Thefts Had A Huge Surge In 2020:** *https://www.tdaniels.com/identity-theft/*

April 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."

Is Your Cyber Security Policy (Or Lack Of One) Leaving You Wide Open To Attacks?

Every business, big or small, should have a cyber security policy in place for its employees. Employees need to know what's acceptable and what isn't when it comes to all things IT. The policy should set expectations, lay out rules and give employees the resources necessary to put the policy to work.

Your employees represent the front lines of your business's cyber security defense. You may have all the antivirus software, malware protection and firewalls in the world, but if your employees aren't educated about IT security or don't understand even the basics, you're putting your business at MAJOR risk.

What can you do to remedy that? You can put a cyber security policy in place. If you already have one, it's time to update it. Then, once it's ready, put it into action!

What does a cyber security policy look like? The specifics can look different from business to business, but a general policy should have all the fundamentals, such as password policy and equipment usage.

For instance, there should be rules for how employees use company equipment, such as PCs, printers and other devices connected to your network. They should know what is expected of them when they log into a company-owned device, from rules on what software they can install to what they can access when browsing the web. They should know how to safely access the work network and understand what data should be shared on that network.

Breaking it down further, many cyber security policies include rules and expectations related to:

Continued on pg.2

Continued from pg.1

- E-mail use
- Social media access
- General web access
- Accessing internal applications remotely
- File sharing
- Passwords

Policies should also break down IT roles within the organization. Who do employees call, text or e-mail if they need IT support? What is the hierarchy they are expected to follow? Do they have internal support? Do they contact an IT service provider like T. Daniels Consulting?

It's important for employees to have resources in order to effectively execute policies. This can come in many forms. It may be a guidebook they can reference or a support phone number they can call. It might be ongoing training on cyber security topics. Or it might be all of the above (as it often is!).

Break down every rule further. Passwords are a great example of an area of policy every business needs to have in place. Password policy often gets overlooked or simply isn't taken as seriously as it should be. Like many cyber security policies, the stronger the password policy is, the more effective it is. Here are a few examples of what a password policy should include:

- Passwords must be changed every 90 days on all applications.
- Passwords must be different for each application.
- Passwords must be 14 characters or longer when applicable.
- Passwords must use uppercase and lowercase letters, at least one number, and at least one special character, such as @, #, % or &.
- Passwords must not be recycled.

The good news is that many apps and websites automatically enforce these rules. The bad news is that not ALL apps and websites enforce these rules – meaning it's up to you to define how employees set their passwords.

Putting a cyber security policy in place isn't easy, but it's necessary, especially these days. More people are working remotely than ever. At the same time, cyberthreats are more common than ever. The more you do to protect your business and your employees from these cyberthreats, the better off you'll be when these threats are knocking at your door.

If you need help setting up or updating your cyber security policy, do not hesitate to contact us at 810-629-0131 or via email at info@tdaniels.com. We can help you put together exactly what you need for a safer, more secure workplace.

"Putting a cyber security policy in place isn't easy, but it's necessary, especially these days. More people are working remotely than ever."

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

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/itbuyguide-421/

Shiny New Gadget Of The Month:

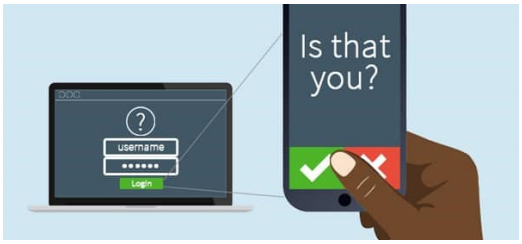
Sticker — The Smallest Finder By Tile

First, there was the Tile – a small, square device used to find just about anything. You attach Tile to the thing you don't want to lose (keys, for example) and you pair Tile with the Tile app. Easy!

Now, Tile has introduced Sticker, their "smallest finder." It's a mini-version of their popular fob, and it can be stuck to just about anything, from TV remotes and portable electronics to tools, bikes, you name it – anything you don't want to go missing.

Plus, not only does Sticker stick to anything, but it also has a three-year battery life, so as they say, "you can set it and forget it." Once it's paired with the smartphone app, it's super-easy to track. And if you lose a "Stickered" device, Sticker emits a loud ring to help you locate your misplaced item, at a range of about 150 feet. Learn more about Sticker at **TheTileApp.com/en-us/store/tiles/sticker**.

How Can Your Business Use the Same, High Level Computer Security, Used By All of the Major Banks?



The answer is MFA. What is MFA?

Cybercriminals have more than 15 billion stolen credentials to choose from. If they choose yours, they could take over your bank accounts, customer records, company secrets, and more.

Multi-factor authentication (MFA) is important, as it makes stealing your information harder for the average criminal.

As the name implies, MFA blends at least two separate factors. One is typically your username and password, which is something you know. The other could be:

- Something you have. A cellphone, keycard, or USB could all verify your identity.
- Something you are. Fingerprints, iris scans, or some other biometric data prove that you are who you say you are.

Adding this secondary factor to your username/password protects your privacy. And it's remarkably easy to setup and use.

Don't Passwords Offer Enough Security?

We all use passwords to gain entry into our email systems, line of business applications, and bank accounts. We are usually forced to change our combinations periodically in the hopes that we'll stay just a bit safer. But the truth is that, on their own, passwords no longer provide an appropriate level of security.

Consider Google. One password gives access to: Gmail, Calendars, YouTube, and other web apps using your Google account as a login method.

In 2017, Google admitted that **hackers steal almost 250,000 web logins each week**. That number is almost certain to be even higher now. And each incident can be incredibly dangerous.

When we think about data breaches, we often think about bank accounts and lost money. But most businesses are a literal treasure chest of customer's personal and financial information and are under constant threat of cyberattacks. And consider this, ransomware attacks will occur every 11 seconds in 2021, according to forecasts from Cybersecurity Ventures.

Benefits of Multi-Factor Authentication

Many organizations have adopted MFA, given the realities of today's security landscape and regulations. With compliance standards like PII and PCI requiring sophisticated security policies, MFA's presence will only continue to become more widespread.

MFA Enables Stronger Authentication

Risk reduction is critical for businesses. In a world where credential targeting is a constant threat and over 80 percent of hacking-related breaches are caused by stolen or weak passwords, this kind of bulletproof authentication solution is essential. It adds another layer of protection from the kinds of damaging attacks that cost businesses millions. A security breach caused by a weak user password would understandably have huge consequences for both your business and your customers.

MFA Offers Security Without Compromising User Experience

There is no question that passwords are a headache to remember — the more users need to remember, the lazier their password habits become. MFA secures the environment, the people in it, and the devices they're using without requiring cumbersome resets or complicated policies.

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. Need more info or help on getting MFA enabled for your business, visit: https://www.tdaniels.com/secure-factor/ or contact us (810) 629-0131 and we will be glad to help.

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 security, cloud expertise and 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 Simple Yet Effective Ways To Boost Employee Morale

Good employee morale is essential to any successful business. It's a reflection of company culture and has a direct impact on not just happiness but also productivity. Here are three surefire ways to improve morale within your organization:

1) Keep The Door Open. When supervisors or management vanish without a trace, it hits morale hard. It's crucial to be present and available to your team. Sometimes it's as simple as keeping the door open, but it also includes having transparent communication. Keep people looped in, especially when there are good things to report on. On top of that, have regular one-on-one chats with everyone on the team and make sure their needs are being met.

2) Emphasize Mental Health. Everyone should have their mental health acknowledged. Always take time to assess the mental health of everyone on your team. If they need to take a break or refocus, make sure they do. If they need a mental health day (or a vacation), encourage it. Be flexible and understanding.

3) Reward And Recognize. Make sure hard work gets recognized and people get credit for that hard work. Shout out star players during meetings and make sure everyone (including management) sees the good work that's being done. And don't hesitate to dole out rewards (lunch, gift cards, etc.) in recognition of that hard work, as well. *Inc., Nov. 4, 2020*

How Big Data Reveals The Humans Behind Your Users

The Internet is a data mine. From search engines to ad clicks, we can see what people are interested in. Big Data is accessible to just about every business, and it can tell you a lot about the people you do business with — or the people you want to do business with.

If you aren't tapping into Big Data (Google Analytics is an example), you're missing out. You can use data to home in on the customers you want to acquire and reduce those costs at the same time. You can better develop products and services you know customers will love. And you'll be able to adapt to changing trends driven by real people. *Inc., Jan. 26, 2021*