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

T. Daniels is holding a FREE Executive Seminar on **"7 Critical IT Security Protections EVERY Business Must Have In Place NOW"** and you are invited!

The seminar is designed for non-technical folks and aimed at owners/ mangers who have questions and concerns about their organization's IT security.

During this seminar, scheduled for February 19th, 2020 you will discover your **#1 security threat,** plus **7 Critical IT Protections YOUR Organization Must Have in Place NOW!** You will also learn the **shocking truth** about bank fraud and why firewalls and antivirus applications give you a **false sense of security**.

To learn more about the presenter and/or register visit our www.tdaniels.com/seminar or call our office at (810) 629-0131.

February 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!"

If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

Continued on pg.2

Continued from pg. 1

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

"The reality is that cyber security should be a normal, everyday part of any business."

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

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 www.tdaniels.com/ITbuyersguide**

Shiny New Gadget Of The Month:

M&R Digital Counting Coin Bank

Many of us still keep a coin jar to toss our spare change into. Even with the growing popularity of apps like Apple Pay and Google Pay, coins remain a big part of our lives. Of course, when you're tossing coins into a jar at the end of the day, you have no idea how much you've collected until you count it or take it to a Coinstar.

The M&R Digital Counting Coin Bank solves this problem. You never have to count change again. Every time you drop coins into the bank, it counts and adds them to the total. The digital readout keeps you updated on how much you've saved. It's a remarkably simple piece of technology that eliminates the hassle of keeping track of change.

3 Reasons Why Recessions Are Awesome For Great Companies

It may be jarring to read the words "recession" and "awesome" in the same sentence. Recessions are bad for most people. I will not make light of how horrible recessions are for the vast majority of companies and their employees, (as well as for not-for-profit organizations and governments).

For most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, increased board and shareholder pressure, increased financial strain and a feeling of looming danger in the pit of your stomach, which is no fun to wake up to every day!

But for great companies, recessions can be awesome.

What are great companies?

Great companies make great products or deliver great services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take great care of customers and employees, great companies don't have a dangerous debt burden. They are profitable and able to pay their bills to suppliers while delivering an attractive return to investors in dividends and equity appreciation.

How are recessions awesome for great companies?

Recessions allow great companies an opportunity to do the following:

1. Shake loose the cobwebs of complacency. "Success breeds complacency," said Andy Grove, the legendary CEO of Intel. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace (*Only The Paranoid Survive*), I am here to suggest that great companies have to keep hustling to stay great.

A recession provides an opportunity for a wake-up call to great companies that may start to coast on past greatness and help them get back on track.

2. Take customers and colleagues away from lesser companies that don't deserve them. As lesser companies stumble during a recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more customers and talented people. I remember when a successful business services company with 70 locations around North America entered the '08 recession. Lesser competitors were closing branches and laying off people, and service was slipping. But the CEO of the successful company was not fearful about the recession. Instead, he sensed the opportunity to win more customers with better service and poach some top talent away from the struggling competitors. The recession allowed this great company to gain market share and build a stronger leadership talent pipeline.

3. Increase the rate of learning of your leaders. Time seems to move more quickly for me during harder times than during easy times. This can improve the learning curve of your up-and-coming leaders. Just remember to not make too many decisions for them; that will stunt their growth. Allow your leaders to come to you with problems and solutions, and coach and support them. Let them test and learn various approaches to leading through uncertain times.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times *best-selling book,* Who: A Method For Hiring, *and the author of the No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*

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.

7 Things To Do So You DON'T Get Hacked When Shopping Online

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

Top Tips For Scaling Security For Your Small Business

Put a greater emphasis on passwords. As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA). MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security. There are many MFA options available for different-sized businesses. Make it a part of your cyber security policy. *Small Business Trends, Nov. 1, 2019.*

Time Has Now Run Out For Windows 7

You have likely heard about the now passed deadline of **January 14, 2020** to have moved your Windows 7 devices to Windows 10. Perhaps you even finished the upgrade across your network before the deadline and if so, congratulations!

However, if you are reading this and have started the process but are unable to complete the project due to the complexity, time, and/or resources required or you haven't even started, we can help. Every device still running Windows 7 at this point leaves you **exposed to serious hacker attacks** aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

To learn more about how T. Daniels Consulting help, simply call us at 810-629-0131 or e-mail us at info@tdaniels.com.