



T. Daniels Consulting

THE T. DANIELS TIMES



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:

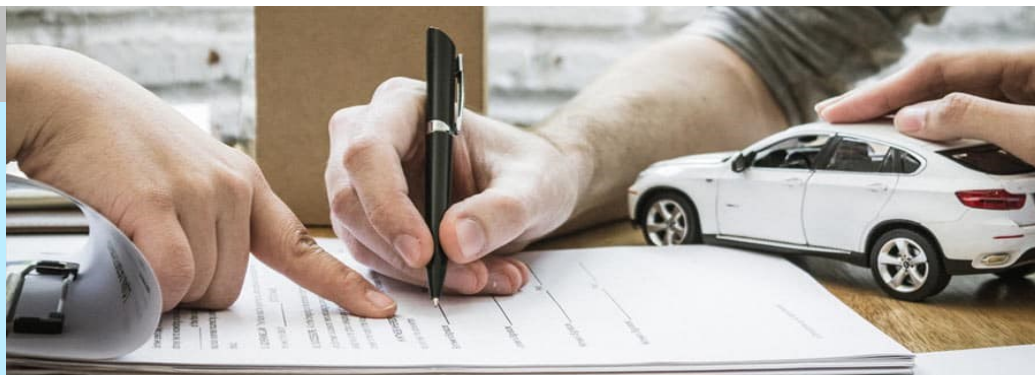
- **Ransomware Attackers Demand 20 Million From US Kia Motors:** <https://www.tdaniels.com/kia/>
- **Saving Money With Microsoft Teams:** <https://www.tdaniels.com/teams/>
- **Finishing First With Renault Sports Formula One:** <https://www.tdaniels.com/renault/>

May 2021



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

“As a dealership 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 Dealership Part of the Reason Loan and Lease Fraud Increased 88% in 2020?

Here is a sobering statistic. Identity theft from **loan and/or lease fraud increased by 88% in 2020**. Let’s put this into further perspective. Debit/credit card/ACH fraud saw only a **32% increase**. Let that sink in. **Loan and/or lease is almost 3 times higher than credit card fraud.**

From VIN numbers to social security numbers, your dealership has extremely sensitive data that is of **high value to thieves and high risk of penalty cost to you**. Your dealership is not immune to the alarming increased threats and hacks that lead to the significant increase in loan and lease fraud last year. **Don’t ignore it!** It is important for managers and owners to keep a strong focus on secure and reliable business operations. Your dealership must protect consumer and employee information, and this requires an effective data security strategy.

Here are 5 critical steps your dealership

should implement as soon as possible to safeguard private information (PII) and develop a strong IT security strategy:

1. **Conduct a network assessment and penetration test (PEN).** This thorough assessment of your network includes things like: identifying vulnerability in your network for access to sensitive data for users that have not worked for the company in years. Or open ports on your firewall that give hackers access to everything. How, because one of your vendors opened it when installing a software update, printer, hand held or the like. What about applications installed on YOUR dealership’s devices? Would it surprise you to learn that you employees have installed social media, pornographic, and/or gambling applications? Not only do these applications waste valuable company time, they also significantly increase your security risks. A PEN Test will simulate an attack on your network

Continued on pg.2

Continued from pg.1

and determine how secure your network really is. With the evolution and sophistication of cybercriminals, it's no longer a question of can your network be broken into, it's a matter of how easy it is to do it..

2. Secure devices and keep non critical functions on a separate network. Dealerships regularly use tablets and computers to access, share, and store information. Limit your risk of a data breach by conducting regular audits of all these devices. It is also important to keep all non-critical functions, like guest wi-fi, on a separate network. This way, if there is a breach at your dealership, your business data won't be affected.

3. Ensure your anti-virus is up to date. Simply having anti-virus installed on your devices is not enough. You must ensure that is updated regularly and automatically. New cyber threats are released daily, sometimes hourly. Your anti-virus needs to be updated real time in order to protect your dealership against these new threats.

4. Define policies and hold everyone accountable. Create cyber security policies for your dealership and your employees. Employees should understand the importance of security and should have processes to follow to ensure the IT environment is secure. Additionally, they should also be clear on what is not allowed with customer data and work computers. Include guidelines on password strength, remote

work and bring-your-own-device (BYOD) options. This establishes a culture of cyber safety at your dealership.

5. Provide security training and make sure EVERYONE completes it. It doesn't matter if it's one time per day or all day long, any employee with access to your dealership's network and customer data is a potential security risk. Hacking techniques continue to get more sophisticated thus, your team needs to continually be trained on how to avoid security issues online. 80% of breaches are caused by human error. It is important employees know how to spot fake "phishing" emails and avoid clicking risky links or downloading an infected attachment.

So, where do you start? You can work with a company like T. Daniels Consulting that specializes in supporting dealerships. We know the nuances particular to dealerships. And because we know the risks that dealerships face, for a limited time, we are offering a chance to win a Network Assessment and PEN Test * (which simulates a real cyber-attack to identify security issues). Visit <https://www.tdaniels.com/assessment/> to take advantage of this limited time offer (**valued at \$15,000-\$30,000***) and be well on your way to securing your most valuable asset, your data.

Win A Network Assessment And Penetration Test (Valued at \$15,000-\$30,000*)



Here is your opportunity to win a Network Assessment and PEN Test. If selected during our chance drawing, our highly skilled team of IT pros will come to your dealership and conduct a Network Assessment and PEN Test (which simulates a real-world cyber-attack to identify security issues) to pinpoint any weak spots in your network.

After the assessment is done, we'll prepare a customized "Report Of Findings" that will reveal specific problems and provide a Prioritized Action Plan for getting these issues and vulnerabilities addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the companies we've done this for discover they are completely exposed to various threats in a number of areas.

Register To Win The Assessment And PEN Test Today At*:

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

*One winner will be drawn by chance drawing. All other registered entrants will receive 50% off a Network Assessment and PEN Test (exact savings will be determined by the size and complexity of your current network.)

Shiny New Gadget Of The Month:



Ember Temperature Control Smart Mug

Porcelain mugs are so 20th century! Meet the Ember Temperature Control Smart Mug – a mug that gives you more options than any mug *ever*.

What's the big deal, you ask? The Ember keeps your drink – coffee, cocoa, tea, milk, etc. – at the exact temperature you want, between 120–145 degrees Fahrenheit. You can also control the mug from your smartphone – adjust the temperature, set notifications and more. The Ember mug is hand-wash safe as well.

The mug itself includes a 1-hour battery to keep your beverage hot on the go, or you can use the included charging coaster to keep your beverage hot all day long. Find the Ember mug on Amazon or learn more at [Ember.com](https://www.ember.com).

3 Questions You Should Ask Any IT “Expert” Before Letting Them Touch Your Computer Network

There are seemingly countless IT services providers to choose from these days, and it can be challenging to tell one from another. However, not all IT services providers are created equal. Some offer independent services, while others are part of larger firms. Some are new to the field, while others have been around for years. There are also companies that put out slick marketing to grab your attention but make it hard to tell if they really live up to the hype.

Well, we're here to help you cut through the clutter. You want to hire someone who knows what they're doing and will take care of your dealership the right way. To do that, there are a few questions you should ask every IT expert before you let them anywhere near your network:

1. What's Your IT Experience?

Education, certifications, and hands-on experience are all important. You want to know your “expert” is actually an expert. It's all too easy for someone to pass themselves off as an expert when they really have limited experience, so you should never hire an individual or a company without vetting them first. After all, this person (or team) will be handling EXTREMELY sensitive hardware and data essential to the operation of your business. This isn't the time to take risks or give someone the benefit of the doubt.

When you work with an IT services company, you can generally expect that the people you work with are educated and experienced, but you should **always** ask. With T. Daniels Consulting, our Microsoft Certified (we have the documentation to prove it!) Professionals and Engineers have an average 10 years' experience which directly benefits you by fixing problems quickly and correctly the first time.

2. What's Your IT Approach?

There are different approaches to IT and network

security. You have the old-fashioned **break-fix** approach and you have the modern **Preventative IT** approach. The break-fix approach used to be the staple of the IT industry and is pretty straightforward: something breaks, so you hire someone to come in and fix it. If many things break or something complicated breaks, you could be looking at a pretty hefty bill – not to mention the costs associated with downtime.

Today, providers like T. Daniels Consulting take a preventative approach (and if they don't, look elsewhere). We don't wait for something to break – we are already on it, monitoring your network 24/7, looking for outside threats or internal issues. We use advanced software that can identify trouble *before* it strikes. That way, we can go to work, proactively protecting your dealership, so you avoid those hefty bills and long downtimes.

3. What's Your GUARANTEED Response Time?

This question often gets overlooked, but it's one that can make or break your dealership. You need to know that you won't be left in the dark when something goes wrong within your network. If you're experiencing a cyber-attack, or a power surge has taken out part of your server, the cost to your dealership can be catastrophic if your IT services provider can't get to you right away.

To learn more about how to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs you didn't anticipate when working with an IT service provider, view our FREE Guide: “The Dealership Owner's Guide To IT Support Services And Fees”. To download, visit: <https://www.tdaniels.com/itbuyguide-dealership/> or give us a call 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.

■ Leverage Good Intel To Beat The Competition

There is a lot of information floating around about your competitors – you just have to find it. When you do, you can give yourself an edge as you put together your own marketing campaigns.

For example, the founder and CEO of Wagmo, Christie Horvath, went as far as contacting and sitting down with a few former employees of her competitors. She was developing a new pet insurance company and wanted to know where those other companies had fallen short. The intel allowed Horvath to innovate and bring new ideas to the table. She didn't copy the competition – she did something different.

Here's another way to approach it: use Facebook's Ad Library tool to watch competitor's Facebook and Instagram marketing initiatives. See what they're doing so you can

do something different and stand out from the crowd. This was something Colin McIntosh, founder of Sheets & Giggles, did, and when he differentiated from his competitors, the customers noticed and flocked to his company. *Inc.*, Jan. 4, 2021

■ A New World Requires New Leadership Skills

Last year marked a major shift in how companies do business. This shift also meant leaders had to change as well. In 2021, adaptation is the name of the game. There are several points leaders have to recognize in their communities and their workforce.

Things won't go back to the way they were. The future will be defined by a new normal. Expectations are different – the expectations of customers and of employees. Buying habits have changed, and work habits have changed. For example, much of the workforce expects a remote or

work-from-home option or greater flexibility from the traditional “9-to-5 at the office” model. If you don't adapt, it may be harder to find qualified employees for your team.

You have to experiment. As you adapt to the changing world, you have to experiment more. This includes your approach to running your business, the products or services you offer, your marketing, hiring practices and so on. Be opening to trying new things, see what works and what doesn't – and let your employees do the same. It's all about encouraging ideas. *Forbes*, Jan. 16, 2021

■ It's Time To Uninstall Adobe Flash Player

On Dec. 31, 2020, Adobe dropped support for their Adobe Flash Player platform. For 25 years, Flash Player had been an integral part of the internet. It gave webpages an extra oomph in the form of interactivity. It came in the form of video, audio, games, buttons and much more. It laid the foundation of what much of the internet is today.

But Flash Player had a dark side. It was a security nightmare. Hackers and cybercriminals routinely exploited Flash and put countless users and websites at risk. Over the years, security experts tried to get people to uninstall Flash, but the platform persisted. Until now. If you still have Adobe Flash on your computer, take a minute to uninstall it.

