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

Wireless network or WiFi—the moment you hear these words you realize how convenient your life has become. Wireless connections have made it easy for anyone to use the internet from any device, including laptops, smartphones, and tablets, etc. from anywhere in the office without managing tons of cable bundles.

One important thing to consider here that wireless network does not end at your office walls, it is possible that the signals of your wireless network are extended through the neighboring area and into other offices. This means your Wi-Fi network is highly vulnerable to hacking.

Learn more about the risks of having an insecure wireless network on **Page 3**, call us at **810-629-0131** or send an email to: **info@tdaniels.com**

September 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!"

Why Your Business Is The PERFECT Target For Hackers...

And What You Need To Do NOW To Protect Yourself

Everybody gets hacked, but not everything makes the evening news. We hear about big companies like Marriott, Twitter, Zoom, and MGM Resorts. What we rarely hear about are the little guys – the small businesses that make up 99.7% of employers in the United States, according to the Small Business Administration. It's these guys who are the biggest targets of cybercriminals.

Basically, if you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cyber security survey by the Ponemon Institute found that 67% of small and midsize businesses in the U.S. and U.K. were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

1. **Small Businesses Are The Most Vulnerable.** Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security can take a back seat to other things, like marketing or customer support. This also means

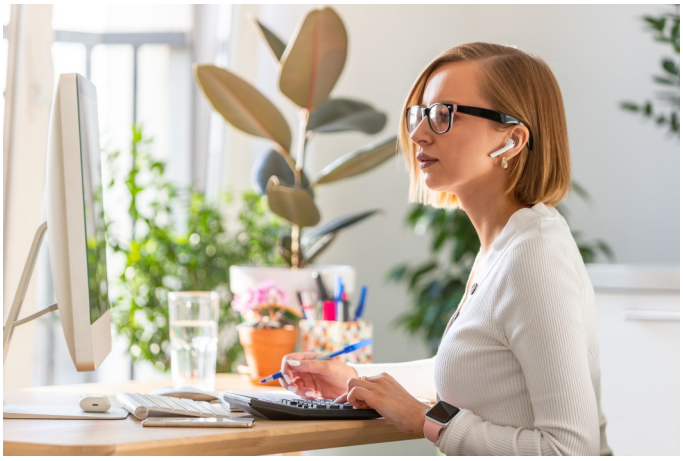
Continued on pg.2

Continued from pg.1

they might not be investing in good network security or any IT security at all. It's just not top-of-mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

2. **Small Businesses Don't Take IT Security Seriously.** Coming off that last point, it's true that many businesses don't properly secure their network because they feel that they *aren't* vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along those same lines, they might not even take password security seriously. According to research conducted by Trace Security, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data, such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

3. **Small Businesses Don't Have The Resources They Need.** Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cyber security, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers



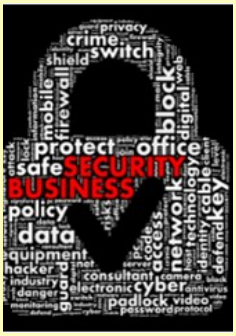
are more confident in attacking these businesses.

Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network 24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything they can to use technology against us, you can use it against them too. Work with a dedicated and experienced IT security firm. Tell them your business's network security needs, and they'll go to work fighting the good fight against the bad guys.

"67% of small and medium-sized businesses in the US and UK were hit by a cyber-attack."

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Small Business, Local Government, or Non Profit Organization

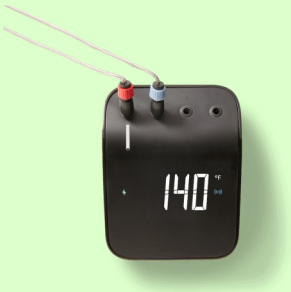


At no cost or obligation, our highly skilled team of IT pros will come to your location and conduct a comprehensive cyber security audit to uncover loopholes in your organization's IT security.

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

Claim Your FREE Assessment Today At:
https://www.tdaniels.com/cyber-security-audit920/
Or Call Our Office At: 810-629-0131.

Shiny New Gadget Of The Month:



Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at **bit.ly/3eTL69Y**!

Business Risks of Insecure Networks

The low cost and easy installation of wireless equipment has made it possible for even the smallest of businesses to set up a wireless network. But just because something is inexpensive and easy doesn't mean that it is the right thing for your business.

Cybercriminals are taking advantage of these scenarios and are focusing their energies on small and vulnerable organizations. An unsecured or inadequately secured wireless network can expose your company to a number of risks including:

Data Loss
Even reading this can give you goosebumps if you are a business owner. Well, they say ignorance is bliss but not in the world of business. There is another saying, what keeps the CEO up at night is not what they know but what they don't know. Most people do not realize that one insecure wireless network can compromise the entire network system. The impact of an insecure wireless network can expose your organization to ransomware and cyber attacks. This can cost you money, customers, and suppliers.

Business Intelligence
Even small businesses have competitors, and unsecured networks create the possibility of an unscrupulous competitor gaining access to your records. With programs freely available from the Internet, anyone can sit in a car outside your place of business and enjoy access to your customer files, accounting data, usernames and passwords, or any other information on the network. A competitor in possession of such in-depth knowledge of your operations can be a damaging or even fatal threat to your business.

Loss of Goodwill
The life's blood of any business is its customers, and their willingness to continue doing business with you. If a cyber attack should compromise your customers' personal or business financial information, or lead to private details becoming public, the repercussions can be serious. Fixing the problem is costly, time consuming, and represents a major inconvenience at best for your customers. At worst, it can cost them a substantial sum. If you gain a reputation as a company that doesn't adequately protect customer data, you've given your clients a strong reason to go elsewhere. You may also leave yourself open to litigation.

Legal and Financial Risks
The legal and financial consequences of a data breach can be significant. Consumers who lose funds to identity theft usually have recourse with their banks, but as a business you might not. More important, your clients, suppliers or other parties might attempt to make good on their losses by suing your company. Lawsuits cost time and money, even if they're ultimately resolved in your favor. A ruling that holds your company liable can be seriously damaging, especially if it exceeds your liability coverage. At the very least, such suits are damaging to your reputation.

T. Daniels Consulting can help evaluate and secure your wireless network. To learn more, visit: https://www.tdaniels.com/securewifi 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.

Back To Basics

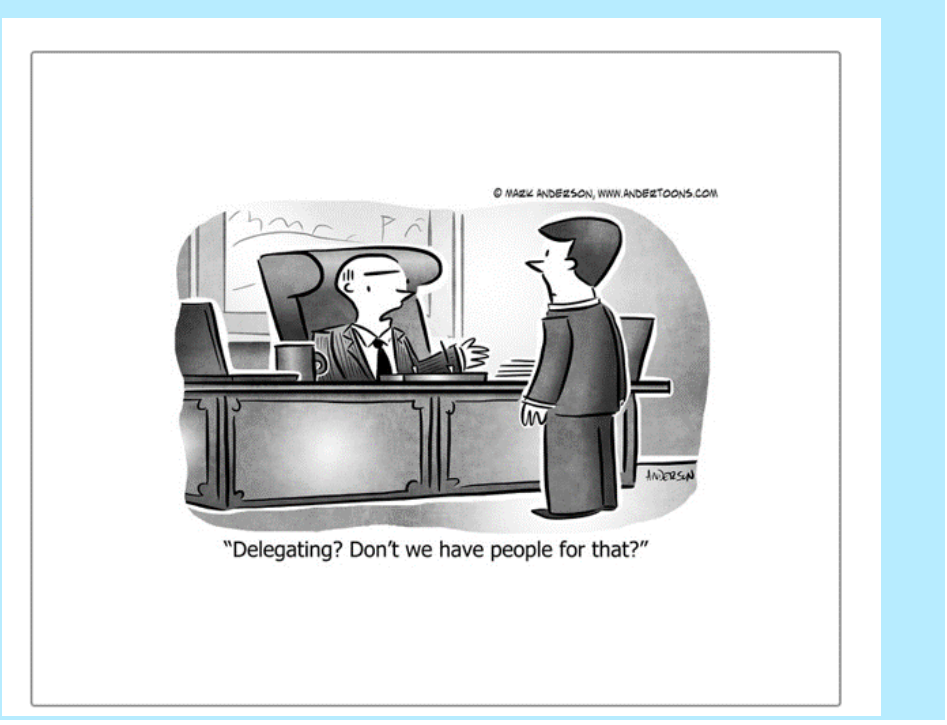
A lot of time is spent staying protected from the newest type of scam or the newest cybercrimes, but as is true with many things, remembering the basics is the entire foundation of making sure you, your company and your clients remain safe.

Everyone in the company or organization should know basic security principles. Security principles and policies should be documented and part of every new employee training. Strong password requirements, Internet usage guidelines and only connecting remotely over VPN are examples of some common security policy items. Strict penalties for violating the security policies should be detailed.

It's not a good habit to save files onto your computer if there is a location on the network or on your server where they can live. They're much less likely to be backed up on your computer, whereas they'll reliably and regularly be backed up if they are saved on the server.

If you use websites or software that do not require regular password changes, set a calendar reminder to change the password yourself every other month.

As with other things, a little prevention goes a long way – remembering the security basics, and asking about them if you don't know what they are, is the single best thing you can do to protect yourself and protect the company.



3 E-mail Productivity Tricks You Need To Know

Turn Off Notifications. Every time you get a ping that you have a new e-mail, it pulls your attention away from what you were doing. It's a major distraction. Over the course of a day, you might get several pings, which can equal a lot of time wasted. Set aside a block of time for reading and responding to e-mails instead.

Use Filters. Many e-mail programs can automatically sort incoming e-mails. You define the sources and keywords, and it does the rest. This helps prioritize which e-mails you need to respond to soonest and which are most relevant to you.

Keep It Short. Most of us don't like to read e-mails – and so we don't. Or we quickly scan for relevant information. Your best bet is to just include the relevant information. Keep it concise and your recipients will appreciate it, and as a recipient, you'll appreciate it as well. *Small Business Trends, April 23, 2020*